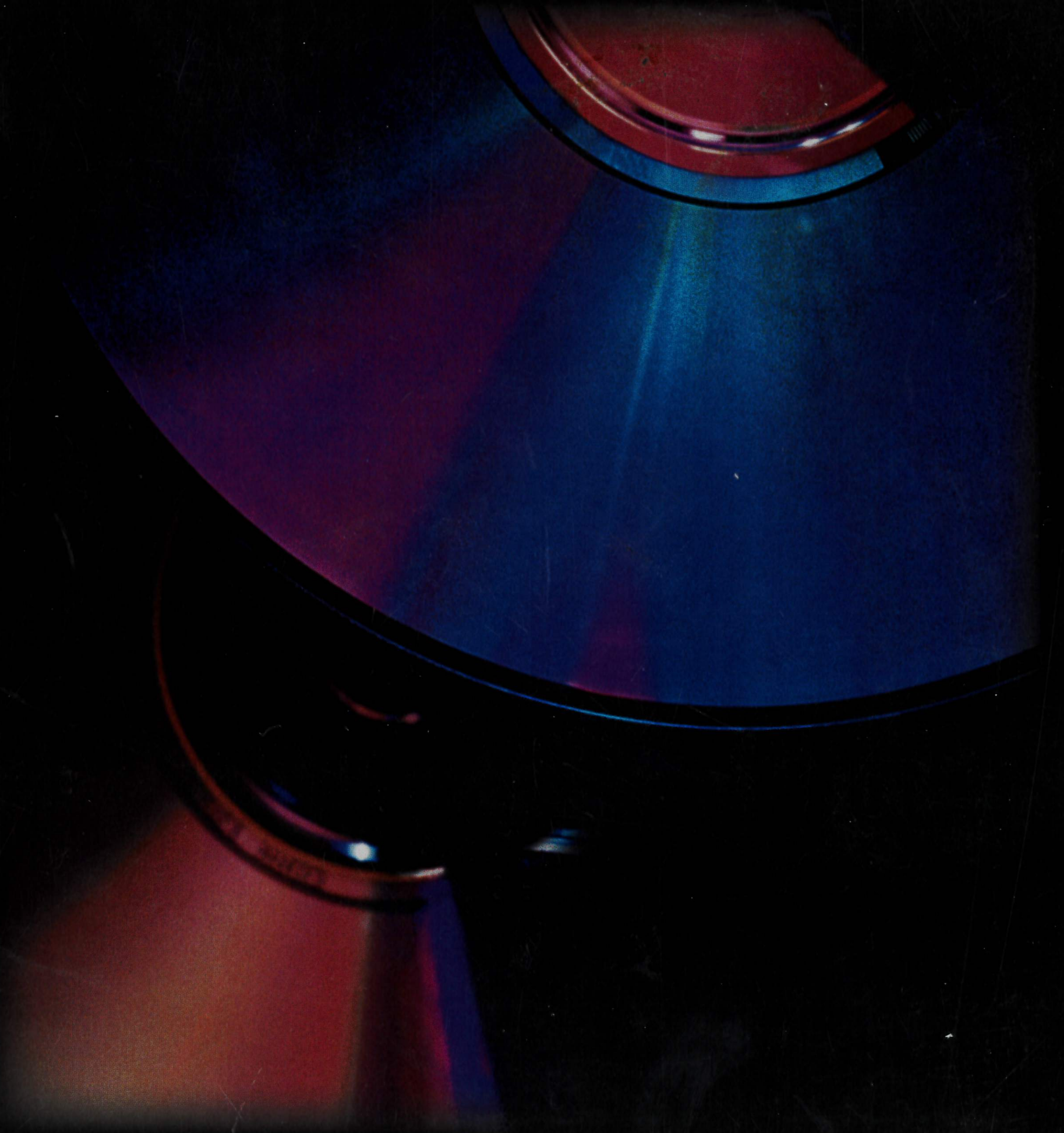
ECLIPSE
DATA TECHNOLOGIES

EclipseSuite BD

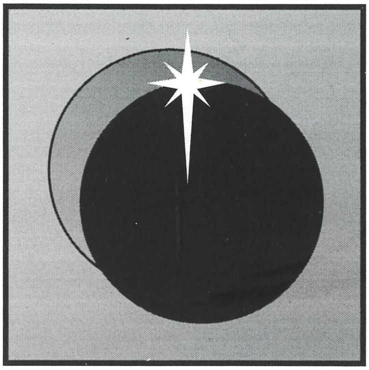
USER'S MANUAL – VERSION 5.0



REVOLUTIONARY OPTICAL TECHNOLOGY MADE SIMPLE

EclipseSuite BD

User's Manual



ECLIPSE
DATA TECHNOLOGIES

Version 5.0

Licensing & Warranty Agreement

You are granted a personal license to use this Software under the terms stated in this Agreement. You may not assign or transfer the Software, the hardware dongle, or this license to any other person without the express written consent of Eclipse Data Technologies. Any attempt to sublicense, assign, or transfer any of the rights, duties, or obligations hereunder is void. You may not copy, modify, alter, electronically transfer, or lease the Software, hardware dongle, or documentation. The license is effective until terminated. You may terminate it at any time by destroying the Software and returning all hardware dongles to Eclipse Data Technologies. It will also terminate if you fail to comply with any term or condition of this Agreement. You agree upon such termination to destroy the Software and return the hardware dongle to Eclipse Data Technologies.

For a period of one year from the date of purchase, Eclipse Data Technologies Inc. warrants that the Software, diskette and hardware dongle shall be free from defects in materials and workmanship under normal use, and agrees to provide you with minor enhancements (i.e., performance improvements to existing basic features of the Software, as opposed to major revisions in Software features). The entire liability of Eclipse Data Technologies, Inc. and your exclusive remedy shall be the repair or replacement of the Software, diskette or hardware dongle not meeting this limited warranty. In no event will Eclipse Data Technologies, Inc. be liable for any damages, including any lost profits, or other incidental or consequential damages arising out of the use or inability to use these products. Eclipse Data Technologies, Inc. specifically disclaims any warranty of any other kind, including any warranty that goods are merchantable or fit for a particular purpose.

This warranty gives you specific legal rights, and you may also have other rights which vary from state to state. This Agreement will be governed by the laws of the State of California.

EclipseSuite BD User's Manual

Part Number: 15-00001
Version 5.0, January 2014

Printed in the USA

All trademarks contained within are property of their respective owners.

Eclipse Data Technologies
5139 Johnson Drive
Pleasanton, CA 94588
USA
Phone: 925-224-8880
Fax: 925-224-8881
www.eclipsedata.com

Eclipse Support
Phone: 925-598-0300
Fax: 925-224-8881
Email: support@eclipsedata.com

Table Of Contents

INTRODUCTION 1

WHAT'S NEW IN ECLIPSESUITE BD 5.0? 2
  Key Features 2
  ImageArchive BD option Enhancements 2
  Miscellaneous Fixes & Enhancements 4
  New Device Support 7
  New BD Rules 7

SYSTEM REQUIREMENTS 9

OPERATING SYSTEM 9
HARDWARE REQUIREMENTS 9
  CPU 9
  Memory 10
  IDE/SATA Controllers 10
  External USB Devices 10
SUPPORTED DEVICES 10
SUPPORTED MEDIA TYPES 11
SUPPORTED FORMATS 11

SOFTWARE INSTALLATION 13

BEFORE YOU BEGIN 13
INSTALLATION 13
  Registry Settings 16
  System Dongle & Key Files 16
  Parallel and USB Ports 17
ECLIPSESUITE SOFTWARE ACTIVATION 17
  Determining if EclipseSuite is Already Activated 17
  Activating EclipseSuite 5.0 BD 19

CERTIFICATE MANAGEMENT UTILITY (CMU) 21

INTRODUCTION 21
  CMU Key Features 21
  CMU Requirements 21
  Installation 22

CONFIGURATION 23

MONITORING FOLDER 23
APPLICATION SETTINGS 23
  General Settings 24
  PGP 26
  Content Certificate 27
  ImageArchive BD 28
  Automation 30

CMU FEATURES 33

CMU MENU 33
  Folder *33*
  View *33*
  Actions *33*
  Window *33*
  Help *34*
CMU TOOLBAR 34
MONITOR FOLDER 35
  Image Path *36*
  Image Type *36*
  AACS Status *36*
  Content Certificate *36*
  Archived *36*
  Signature *36*
  UDFLogVol_ID *36*
  Modified *36*
  Process *36*
MONITOR TASKS 37

COMMON CMU TASKS 39

EXTRACTING THE CC FOR SIGNING 39
SIGNING AN IMAGE 40
  Automatic Mode *40*
  Manual Mode *41*
  Updating File Checksums *43*
CONVERTING A TYPE C IMAGE BACK TO A TYPE B 43
UPDATING MKBS FOR A TYPE C IMAGE 43
CMU LOGS 45

PGP SETUP 47

OPERATION 49

MANUAL OPERATION 49
  Extracting AACS Files for Signing *49*
  Signing an Image *49*

TROUBLESHOOTING 51

RE-USING ENCRYPTION KEYS 53

GENERATING THE ENCRYPTION KEYS AT AUTHORING 53
  Embedding Title Keys in Image *54*
  Using Keys from External File *54*
  Re-Using a Type C Image *54*
  Using Encryption Keys from Existing Image *54*
D IMAGE REQUIREMENTS FOR RE-ENCRYPTING USING SAME SIGNED-CC. 55
  Process *55*
  Result *55*

IMAGEARCHIVE BD 57

RULES & EXCLUSIONS 59

This page has been left blank intentionally.

Introduction

EclipseSuite puts control of the BD pre-mastering and quality control process into the right hands; yours. EclipseSuite is a set of tools that takes the mystery out of BD production problems and introduces a new level of pre-mastering flexibility, data protection and quality control. EclipseSuite is comprised of the following components:

- **ImageAnalysis** – A format checker and image prescreening tool.
- **ImageCopy** – A copying utility used primarily to analyze and transfer images for mastering.
- **ImageVerify** – A QC utility used primarily to compare a replicated disc to the original source image.
- **ImageUtilities** – An assortment of advanced tools that support the main EclipseSuite programs.
- **Plug-In Manager** – A built-in utility that support the use of copy protection Plug-Ins.
- **Advanced Features** – An assortment of advanced features that can be used with the EclipseSuite programs.

Based on Windows XP and Windows 7, EclipseSuite provides the highest level of multitasking and networking available. One operator and one workstation can perform all tasks needed in a typical pre-mastering department by running multiple concurrent sessions of any of the EclipseSuite pre-mastering tools.

All EclipseSuite tools allow user-selectable error, warning, and information events to provide for a Go/No-Go operation based on those settings. The events can apply to format specifications or exclusions. Results can be printed-out and/or saved to a disk file for future reference.

EclipseSuite BD User's Manual

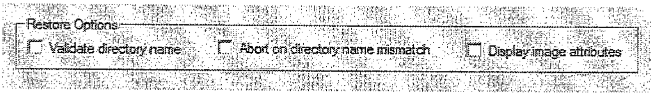
What's new in EclipseSuite BD 5.0?

Key Features

- Enhancements to ImageArchive BD option and new BD Restore Only option feature
- Added log file naming preferences to ImageAnalysis and ImageVerify to reduce operator input.
- Enhanced Royalty Report filename preferences
- Support for Resizing BD type P dual layer images.
- Support for the new Fox Derivative CMF Configuration specifications dated on June 6th 2013
- New Device Support

ImageArchive BD option Enhancements

1. New Preference settings



Restore Options

☐ Validate directory name ☐ Abort on directory name mismatch ☐ Display image attributes

- 'Validate directory name'

  If ImageCopy is restoring an image and the output directory does not match the base directory stored in the database, prompt for action.

  In many cases, the image directory is used as an image unique identifier. When a BD image is archived, its source full path is also stored in the database. When the image is restored, ImageCopy will prompt the user if the chosen output directory does not match with the original directory.

  This directory validation occurs only when the option 'Validate directory name on restore' is selected in the 'ImageArchive BD' preferences of ImageCopy.

  When using ImageVerify to compare a replica to a BDCMF image, the directory can also be validated. This function can be enabled with the option 'Validate directory name' in the ImageVerify preferences.

- "Abort on directory name mismatch" and "Display the image attributes"

  These settings are located in the ImageCopy 'ImageArchive BD' Preferences.

  - *'Abort on directory name mismatch'* is used on a restore operation to alert the user when the output image directory does not match the directory of the archive record. This is useful for customer that use the directory name as the unique identifier of an image. Specifying a different name can lead to problem later in the process if the image directory name is used in the mastering/replication process.

  - *'Display the image attributes'* will display a window prior to the start of a restore operation, which will show image attributes such as the signature, Volume ID, MID and the original directory name. This gives the user a chance to validate that they are restoring the correct image.

2. When archiving and restoring a BD image, there must be 2 public keys and one of them must be the Eclipse key.

   When an image is archived, part of the data is encrypted using an encryption key that was installed with the ImageArchive BD option. The key is unique to each company. A second key is installed for backup purposes. However, the second is a global Eclipse key.

   The keys play an important part in the archive and restore operations. In some cases, however, these keys are removed from the Windows Personal key store and archiving and restore operations may fail. The EclipseSuite tools will now confirm that both keys exist and if they do not, they will be installed from the EclipseSuite installation directory.

3. If doing an ImageArchive restore and the BDCMF data can't be found in the database, use the BDCMF that ImageCopy creates instead of aborting the whole operation.

   Early versions of the ImageArchive BD database did not include the contents of the BDCMF.CMF file. If running a recent version of ImageCopy to restore an old image that did not include this in the database, it would result in an abort. This new version of ImageCopy will, instead, use the BDCMF information created during the pre-scanning of the replica.

4. ImageCopy now prevents restoring from a BD replica if ImageCopy is being executed in a remote desktop connection.

5. When restoring from replica, ImageCopy will now create the FAI.DAT file which is required for BDCMF 1.01 and later.

6. When restoring from replica, ImageCopy will now create the PACL1.DAT file for BD50.

   Although it is optional, some tools require this file to be included.

7. Allow archiving of BDCMF images to recordable media with the 'BD Restore Only' dongle option.

   Initially, this option only allowed restore operations. Now users can also create archives.

8. New Gear libraries have been updated for better performance when creating BD and DVD archives.

9. Support incremental archives of Blu-ray images and also to Blu-ray recordable media for all image types.

10. Increase usable space for non-incremental archives to 98% from 90% for all media and formats.

    Previous versions of EclipseSuite would reserve 10% of the media's capacity for storage of miscellaneous files such as the ImageCopy logs. This would sometimes cause ImageCopy to abort an archive operation indicating that there was not enough space on the output medium if the size of the image being archived was between 90% and 100% of media's capacity.

11. Enhanced ImageCopy to check the recordable media capacity for incremental archives. If there isn't enough space on the output media, display a more meaningful error rather than the generic 'aborted' error.

12. Enhanced the ImageArchive BD option by adding registry parameters that will enable logging of information that can be used for troubleshooting when problems occur.

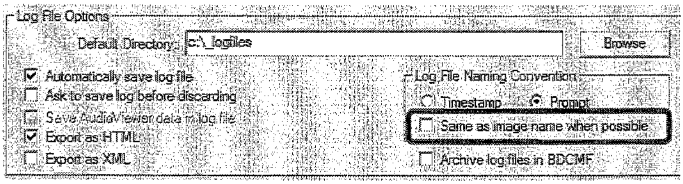
    The following registry settings must be enabled.

HKEY_CURRENT_USER\SOFTWARE\Eclipse\ImageCopy\Settings\ArchiveDbg
HKEY_CURRENT_USER\SOFTWARE\Eclipse\ImageCopy\Settings\ArchiveDbgDir

Both parameters should be of type REG_SZ where ArchiveDbg is set to 'YES' to enable the debug logging and ArchiveDbgDir is the set to the directory where the logs will be created. Some or all of the following files will be generated: CPY_BD.log, DI.log, NV_BD.log, RI.log, WRTCD_BD.log and NT.log

Miscellaneous Fixes & Enhancements

13. Added log naming option "Same as image name when possible" to the Preferences in ImageAnalysis and ImageVerify. This saves the operator from the need to type a log file name, or cut and paste it from the BDCMF image directory name.



Log File Options
Default Directory: c:_logfiles
☑ Automatically save log file
☐ Ask to save log before discarding
☐ Save AudioViewer data in log file
☑ Export as HTML
☐ Export as XML
Log File Naming Convention
○ Timestamp ● Prompt
☐ Same as image name when possible
☐ Archive log files in BDCMF

14. Added new warning rule "No Playing Time specified".

    This rule will be triggered if the PlayingTimeInfo element is not specified in the BDCMF.CMF file. In previous versions, this element was not required. In current versions, however, it is required. Previously this was reported with a general error message. In this version, this new rule will be triggered instead allowing users to change the severity to INFO or other less severe level since it does not affect the processing of images with this problem.

15. Added rule "BD+ SVM file contains all zero".

    This rule is triggered if a *.svm file in the BDSVM directory contains all zeroes. This only applies to non-Type V images after the BD+ process.

16. Added rules "BD-Video" and "BD-Data".

    These rules are triggered according to the Content Category element in the BDCMF.

17. "Invalid UDF version" rule severity changed from Warning to Error.

    Formats such as DVD-Video and Blu-ray require specific versions of the UDF File System.

18. Renamed the rule "File Allocated on the wrong layer" to "Blu-ray AACS File on layer 0" to be consistent with the other "Blu-ray AACS File on layer 1".

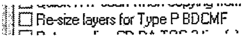
19. Added rule "Application location at layer break". This rule shows the first clip data address after the layer break of a BDCMF image.

20. Identify a BDCMF Type C as 'Type C' rather than 'Type C2' in the Info | BD-ROM tab.

21. Report an error if the UDF file system is not found in a BD image.

22. Corrected a problem in ImageVerify where the HTML log does not display the behavior file name and target rule file names correctly.

23. Support for resizing the layers of a BD Type P image via a new Behavior.

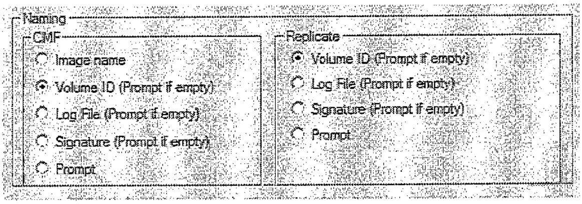


☐ Re-size layers for Type P BDCMF

In mastering and replication, it may sometimes be difficult to process a BD layer if it is filled to capacity. In cases where layer 0 is filled to capacity but layer 1 is not, the new behavior 'Re-size layers for Type P BDCMF' allows ImageCopy to modify the image and balance the data between layers by moving some of the data into layer 1, thereby, ending layer 0 earlier. Note that once the layers are resized, the original source image can no longer be used for comparison to the output or replicates.

24. Corrected a problem in ImageVerify where the royalty report is not generated in the central location if the Source input is a Signature File or Signature Value.

25. Enhanced Royalty Report preferences to have the options of naming the files based on the log filename or the signature.



Naming

CMF
○ Image name
● Volume ID (Prompt if empty)
○ Log File (Prompt if empty)
○ Signature (Prompt if empty)
○ Prompt

Replicate
● Volume ID (Prompt if empty)
○ Log File (Prompt if empty)
○ Signature (Prompt if empty)
○ Prompt

There is also an option to save the royalty report to a Comma Separated Value file (CVS). The following is the syntax of the registry entries to be added in order to enable this option in the EclipseSuite applications. You can copy the text into a file with a *.reg extension. Then you can double-click on the file to add the settings to the registry.

```
Windows Registry Editor Version 5.00
[HKEY_CURRENT_USER\Software\Eclipse\ImageCopy\Settings]
"SaveToCSV"="Yes"
[HKEY_CURRENT_USER\Software\Eclipse\ImageAnalysis\Settings]
"SaveToCSV"="Yes"
[HKEY_CURRENT_USER\Software\Eclipse\ImageVerify\Settings]
"SaveToCSV"="Yes"
```

26. Removed "Single File" checkbox from Royalty Report Preferences as it was unused.

27. ImageCopy now uses the output image name for the royalty report filename when the option "Same as image name when possible" is selected in the Preferences.

    Previously it would default to the source input image name. If the output is a recordable, then the royalty report will use the input name instead.

28. Corrected a problem in ImageCopy where the royalty report will not be created in the output folder if Verify-After-Copy is disabled.

29. Corrected a problem in ImageCopy where the royalty report file was not being generated for BD images when the behavior "Verify using Signature file" was enabled.

30. Enhanced ImageCopy so that during a Verify-After-Copy operation ImageCopy will not be using data from the Windows File Cache for comparison. This will force Windows to read the source/target images instead of using cached information.

    For performance reasons, Windows caches data to file. If this data is needed later, Windows uses the data from the cache instead of re-reading from the original source. This feature is not suitable for the processing of images since it could cause the EclipseSuite tools to not detect media errors.

31. Corrected a problem in ImageCopy where the completion dialog does not show up.
32. Signature file extension "esg" is now automatically appended to the name of a signature file if the input device in ImageVerify is a Signature File and the name does not have an extension.
33. Added index numbering to the extents for Clip AV Information under the BD ROM category in the Info tab.

    The extents displayed in Info | BDROM are identified with an index number and displayed as "Index #". This is done for easy identification and for display purposes only.

34. Corrected a problem where the "Retry Scanning TOC" behavior was being triggered with BD discs.
35. ImageCopy no longer copies *.map files to the output directory if the file is not a copy protection script file.

    Some authoring applications create a *.map file in the image directory. The file is delivered along with the image. The Eclipse software uses *.map files for certain copy protections. When they encountered the *.map file created by the authoring application, it resulted in errors since the structure of the file did not match that of the *.map file used by copy protections. ImageCopy will now validate the content prior to analyzing and transferring this file.

36. Always display the rule "Dual-Layer (Opposite track path) for BD dual layer since there is no PTP.
37. Corrected a problem in ImageCopy where rules and behavior files set via the DCOM interface are not applied to the job.
38. Corrected a problem that was causing log files to fail to load.

    The ISO9660 debug information will not save the ISO tag as hex code instead of string because it is possible for the tag to have 0x1A which is interpreted as EOF, thereby, causing log parsing errors.

39. Corrected a problem where log saving errors aren't displayed.
40. Add additional space for device name display in ImageAnalysis and ImageVerify.

    The ImageAnalysis and ImageVerify boxes where the devices are listed are now wider to support longer device names.

41. Do not add a device to the list of EclipseSuite devices if no drive letter is found.

    This only applies when running in SCSI Pass-through mode. This solves a problem where the address settings in the registry entry for a device don't match the settings retrieved directly from the device.

42. Corrected a problem in ImageCopy where the OUT DDPID and OUT DDPMS Info tab sections were displayed for BD images.
43. Always save the PACL0.DAT file in 64k size packs when a valid PAC is returned but with shorted size.

    Some drives return a valid PAC but with a size less than that of a PAC structure.

44. Corrected a problem in ICheck where the **/c** command line option was not working.
45. When validating the BDCMF.CMF version number, make sure that it includes the correct number of decimal digits to the right of the decimal point.

46. Corrected a problem where the HDMV Region playback analysis is stuck in an infinite loop which eventually causes the application to crash for certain images.

47. Remove excessive debug messages that may be triggered during HDMV analysis.

48. Don't do extent size check on last extent of a SSIF file of a 3D image.

49. Do not use the SetOutputMode command to identify a 3D Blu-ray image.

    This was causing non-3D images to be incorrectly identified as 3D.

50. Changed the BD-Live, BD-3D and BD-Java flags shown under the BDCMF section of the Info | BD-ROM to be the original values from the BDCMF file.

    These flags were supposed to represent the original source image settings. Unfortunately, the EclipseSuite tools were incorrectly displaying the 'corrected' flag values.

51. Add the ability for users to select between SCSI Pass-through (SPTI) or ASPI interfaces.

    The EclipseSuite tools can use ASP or SPTI to command devices for any operation. This is actually a function of the Windows operating system. ASPI was used in older Windows versions. In Windows XP, support for SCSI Pass-through Interface was added. In Windows 7, only SCSI Pass-through Interface is supported.

    Most new devices will use SCSI Pass-through Interface. Therefore, if using Windows XP, users can force the EclipseSuite tools to use SCSI Pass-through Interface or ASPI via the registry.

    \HKEY_LOCAL_MACHINE\Software\Eclipse\EclipseSuite
    Key Name: ForcePassThrough
    Type: REG_DWORD
    Value: [0 = SPTI] or [1 = ASPI]
    Default: 0

    Note that in Windows 7, this parameter has no effect since the EclipseSuite tools will always use STPI regardless of this setting. The only exception is for Tape drives where it will still use ASPI. However, note that in Windows 7 64-bit, tape drives may not work since there is no 64bit ASPI driver support.

New Device Support

- Hitachi-LG 'HL-DT-ST BD-RE BE14NU40' (external USB) and 'HL-DT-ST BD-RE WH14NS40' as a BD readers/writers.

  While these drives are recognized as both readers and writers, Eclipse has only tested them as readers. This is not to say that they do not work as writers but it is something that has not been tested yet.

- Pioneer BD-RW BDR-207 and 208 drives as BD/CD/DVD readers and writers

New BD Rules

Rule Title	Severity	Category	Rule ID
Application location at layer break	Info	Blu-ray	1891
BD Type P Layers resized	Flag	Blu-ray	1899

BD+ SVM file contains all zero data	Error	Blu-ray	1887
BDCMF Type P TL	Info	Exclude	1900
BD-Data	Info	Exclude	1888
BD-Video	Info	Exclude	1889
ImageArchive BD base directory does not match target	Flag	Blu-ray	1893
ImageArchive base directory overridden	Flag	Blu-ray	1894
Missing BDCMF LayerInfo L1SectorSize attribute	Error	Blu-ray	1901
No Playing Time specified	Warning	Blu-ray	1903
Triple layer (Opposite Track Path)	Info	Exclude	1902

System Requirements

EclipseSuite does not require any custom hardware or additional software. The following is a list of minimum software and hardware requirements to run EclipseSuite.

Operating System

The EclipseSuite tools run under **Microsoft Windows 7 Professional and Ultimate** and **Microsoft Windows XP Professional**. In Windows 7, EclipseSuite will run in both 32-bit and 64-bit editions.

The Windows operating systems were selected for their multitasking capabilities. This allows multiple jobs to run concurrently. You are only limited by the speed of the computer, the number of devices available and the amount of memory installed on the computer.

NOTE
Eclipse no longer supports the Windows NT or Windows 2000 operating system.

Hardware Requirements

Most Blu-ray drives use the SATA interface. In some cases, the drive manufacturers will also release the same drive in an external USB enclosure.

EclipseSuite will run on most Pentium computers that meet the minimum requirements listed below. However, if you are using a PC with Windows 7, make sure that it meets at minimum the hardware requirements of that operating system.

Table 1: Minimum Hardware Requirements

Item	Minimum Requirement
CPU	PC with Intel Pentium 4 1.5GHz or faster
Memory	1GB of RAM
Hard Disk	50MB of hard disk space for the EclipseSuite software
SATA PCI Controllers	Adaptec® ASH-1205SA, Promise® TX4 SATAII 150

Hardware requirements vary depending on how you plan to use the EclipseSuite software. For example, if you will be using the system as a loading station, then it is likely that you will need to run several ImageCopy jobs at the same time. This may require a system with more memory, a faster CPU and the appropriate controller for the devices (SATA controllers).

CPU

Although the EclipseSuite software will run on a PC with an Intel Pentium 233MHz PC, it is not practical for a BD pre-mastering and mastering environment. Performance will suffer, especially if using internal IDE or SATA devices. It is recommended that a PC with minimum 1.5GHz CPU be used.

NOTE
If you plan to run more than one job a time, you might consider using a system with a faster CPU and more memory. If you will be copying images to the local hard disk, you might consider getting additional storage capacity.

Memory

If multiple jobs will be run at the same time, it is recommended that you install additional memory on the PC as it will help performance. Windows normally reserves some memory for its own use. Whatever is left over is used by the applications and services that are run. If you run out of physical memory, Windows will cache information to the hard disk as it switches between applications. Since hard disks are much slower than memory, performance will suffer greatly if this occurs. Make sure that you have more than enough memory to support the number of applications that you will be running. If running several jobs at the same time, at least 1GB of RAM is recommended.

IDE/SATA Controllers

All newly supported devices use SATA or USB interfaces. These can be connected directly to the motherboard's SATA onboard controllers or via a PCI SATA controllers if your motherboard is not equipped with any or does not have enough USB/SATA input connectors.

Eclipse has tested the controllers mentioned in Table 1. However, it is possible that other controllers will work as well. Note also that most new motherboards no longer include an IDE connection.

External USB Devices

While most of the supported devices are internal SATA interface, some drive manufactures will often release the same drive in an external USB enclosure. Refer to the list of supported peripherals to see which drives, if any, are external USB interface.

Supported Devices

All devices are commercially available and do not require any special modifications.

NOTE
In keeping the lists of supported devices current, some of the obsolete devices have been removed from this list. If you have a question regarding a specific device not listed here, contact Eclipse Customer Support.

Table 2: Supported Blu-ray Drives

Model	Read/Write Capabilities	
Plextor	**Read**	**Write**
PX-B310U	Y	N
PX-B320SA	Y	N
PX-B940	Y	N
PX-LB950SA	Y	N
PX-LB950UE	Y	N
Pioneer		
BDR-205	Y	Y
BDR-206	Y	Y
BDR-207	Y	Y
BDR-208	Y	Y
Others		
iHES312*	Y	N
HL-DT-ST BD-RE WH14NS40	Y	N
HL-DT-ST BD-RE BE14NU40	Y	N
LG 'HL-DT-STBD-RE WH12LS30 1.00'	Y	N
LG BD HL-DT-STBD-RE BH10LS30	Y	N
MATSHITA BD-MLT SW-5583	Y	N
MATSHITA BD-MLT LF-PB271	Y	N
MATSHITA BD-MLT LF-PB371	Y	N

* *Limited testing has been done with this drive.*

Supported Media Types

The following is a list of all media types supported by **EclipseSuite**:

- BDCMF image
- Sony CMF image
- Blu-ray replica
- BD-R
- BD-RE

Supported Formats

The following is a complete list of all Book/Formats supported by **EclipseSuite**:

- Blu-ray Video
- Blu-ray ROM

This page has been intentional left blank.

Software Installation

Before You Begin

Before installing the EclipseSuite software, make sure the minimum system requirements, as described in the previous section, are met.

EclipseSuite requires a dongle activation. Therefore, if upgrading from a previous version, the dongle may need to be activated to run the new version. If this is a first-time installation of the EclipseSuite software, then it should already be activated. If upgrading from a previous version, Eclipse recommends leaving your existing version until EclipseSuite BD 5.0 has been activated and is operational. Refer to section **EclipseSuite Software Activation** on page 17 for more details.

To install EclipseSuite, the following items are required:

- EclipseSuite Installation Software – The EclipseSuite installation software can be downloaded from Eclipse's FTP site.
- Dongle Key Files – The dongle key files are distributed on a USB thumb drive. The key files are unique to each dongle. If upgrading from a previous version, the installation will use the key files from the existing key file directory.
- EclipseSuite Dongle – The dongle is a hardware key that is used for licensing control of the EclipseSuite software. If you are upgrading from a previous version, the dongle should already be installed. If it is a first time installation, then a new dongle should have been provided.
- Windows Workstation Computer – Computer equipped with the necessary software and hardware as described in the System Requirements section.

Installation

In order to install EclipseSuite you must be logged on to Windows with Administrator privileges so that the setup program can properly alter the registry.

To install EclipseSuite:

1. Logon to Eclipse's ftp site and download EclipseSuite BD 5.0. Note that there are two files available for download: **esbd50.exe** and **esbd50a.exe**.

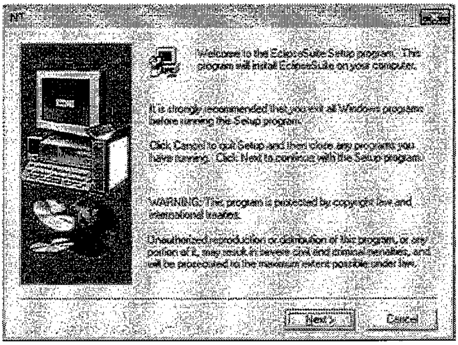
   If you are running with the ImageArchive BD option, then you should download **esbd50a.exe**. Otherwise, download the file **esbd50.exe**.

   NOTE
   *The **esbd50a.exe** and **es50.exe** files are self-extracting executable files. When you run these programs, the installation starts automatically. If you prefer, there are also ZIP versions of these tow files available on the ftp site (**esbd50a.zip** and **esbd50.zip**).*

2. If you downloaded the self-extracting executable file, double-click on it to start the installation.
3. If you downloaded the ZIP file, extract it to a local folder then double-click SETUP.EXE.

> **NOTE**
> *If you are running under Windows 7, you must right-click on the SETUP.EXE program and select* ***Run As Administrator.***

4. The following window will appear recommending that you exit all Windows programs before continuing with the installation. Click **Next** when you are ready to proceed.



NT

Welcome to the EclipseSuite Setup program. This program will install EclipseSuite on your computer.

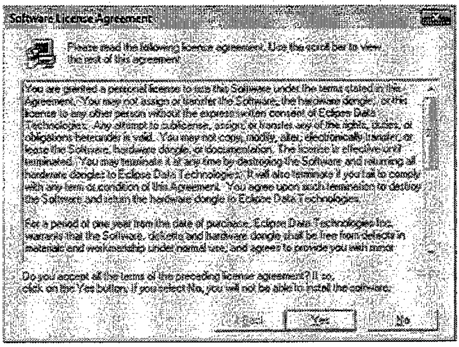
It is strongly recommended that you exit all Windows programs before running this Setup program.

Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

5. Make sure that you read the **Software License Agreement**. If you accept, click **Yes** to continue.



Software License Agreement

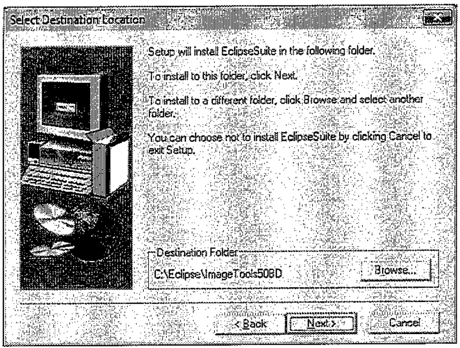
Please read the following license agreement. Use the scroll bar to view the rest of this agreement.

You are granted a personal license to use the Software under the terms stated in this Agreement. You may not assign or transfer the Software, the hardware dongle, or this license to any other person without the express written consent of Eclipse Data Technologies. Any attempt to sublicense, assign, or transfer any of the rights, duties, or obligations hereunder is void. You may not copy, modify, alter, electronically transfer, or lease the Software, hardware dongle, or documentation. The license is effective until terminated. You may terminate it at any time by destroying the Software and returning all hardware dongles to Eclipse Data Technologies. It will also terminate if you fail to comply with any term or condition of this Agreement. You agree upon such termination to destroy the Software and return the hardware dongle to Eclipse Data Technologies.

For a period of one year from the date of purchase, Eclipse Data Technologies Inc. warrants that the Software, diskette and hardware dongle shall be free from defects in materials and workmanship under normal use, and agrees to provide you with mmcu

Do you accept all the terms of the preceding license agreement? If so, click on the Yes button. If you select No, you will not be able to install the software.

6. By default, the setup program will install the EclipseSuite software in the directory **C:\Eclipse\ImageTools50BD**. We recommend that you accept this default setting and click **Next** to continue.



Select Destination Location

Setup will install EclipseSuite in the following folder.

To install to this folder, click Next.

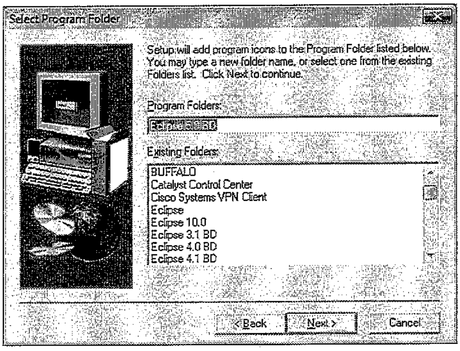
To install to a different folder, click Browse and select another folder.

You can choose not to install EclipseSuite by clicking Cancel to exit Setup.

Destination Folder

C:\Eclipse\ImageTools50BD

7. The setup program will also create a new program group called "Eclipse 5.0 BD". Click **Next** to accept and continue.



Select Program Folder

Setup will add program icons to the Program Folder listed below. You may type a new folder name, or select one from the existing Folders list. Click Next to continue.

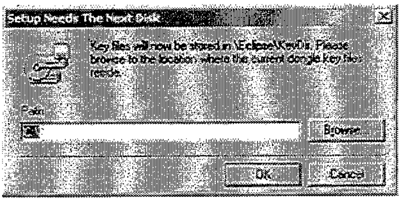
Program Folders:

Eclipse 5.0 BD

Existing Folders:

BUFFALO
Catalyst Control Center
Cisco Systems VPN Client
Eclipse
Eclipse 10.0
Eclipse 3.1 BD
Eclipse 4.0 BD
Eclipse 4.1 BD

8. If you are installing EclipseSuite for the first time, you will be prompted for the dongle Key Files. Browse to the folder where the keys are located and click OK to continue.



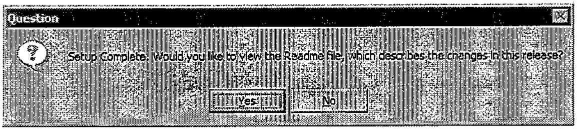
Setup Needs The Next Disk

Key files will now be stored in \Eclipse\KeyDir. Please browse to the location where the current dongle key files reside.

Path:

If you are upgrading, you will not be prompted as long as the dongle key files are present in the pre-configured directory.

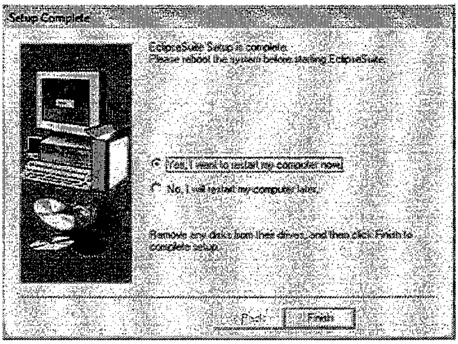
9. At the end of the installation, the setup program will ask if you want to view the **README.WRI** file. We encourage you to read this file as it contains a list of fixes and enhancements since the last release.



Question

Setup Complete. Would you like to view the Readme file, which describes the changes in this release?

10. To complete the installation, the setup program may require you to reboot the computer. If prompted, click Finish to reboot.



EclipseSuite Setup is complete.
Please reboot the system before starting EclipseSuite.

● Yes, I want to restart my computer now.

○ No, I will restart my computer later.

Remove any disks from their drives, and then click Finish to complete setup.

Registry Settings

The following settings are made automatically to the system registry when the software is installed.

CAUTION It is not recommended that you alter the registry settings manually. Doing so may cause your system to become unstable or inoperable.

- **Large System Cache**

  The large system cache is enabled is enabled by default on most computers. It allows the system to use all available memory (and virtual space) for caching of disk file I/O. This has very undesirable performance penalties when copying large files (such as image files). Therefore, this feature is disabled during the installation.

- **AutoPlay**

  When a BD/CD/DVD disc is inserted into a drive, the **AutoPlay** feature of Windows will typically start running the software installation program on the CD-ROM, or, in the case of an audio CD, it will start playing the CD. These actions interfere with EclipseSuite's usage of the drive, and in the case of a CD-ROM, it can start the installation of unwanted software. To avoid this behavior, the AutoPlay feature is disabled the first time that you run any of the EclipseSuite tools.

NOTE
The EclipseSuite tools will automatically attempt to alter the registry setting. However, if the user who is currently logged in does not have Administrator privileges, the program will not be able to make the necessary changes.

System Dongle & Key Files

The dongle is a hardware key that connects to the parallel or USB port on the back of your computer. It is a licensing control hardware key that needs to be connected when running any EclipseSuite application. The key files are generated at the time the dongle is programmed and are unique to each dongle. When any of the EclipseSuite programs are run, they check to make sure that the dongle is connected and that the key file associated with the program you are running is present. For this reason, you should make sure that the key files are stored in a safe place in case the software needs to be re-installed. There should be a key file for each of the EclipseSuite programs that the dongle was programmed for: ImageCopy, ImageAnalysis and ImageVerify. In addition, you may also have a key file for any add-on option such as ImageUtilities. The key files have the same name as the program they represent but have a .key (e.g. ImageAnalysis.key) extension. The ECLIPSE.KEY file, which stores any EclipseSuite option, will also be present.

If installing EclipseSuite for the first time, the setup application copies the dongle key files to a common directory called `C:\Eclipse\KeyDir`. If upgrading from a previous version, you will not be prompted for the key files as they will be used from their preconfigured location.

Parallel and USB Ports

Eclipse uses two types of dongle interfaces: Parallel and USB. If you are using a dongle with a parallel interface, it should be connected to the first parallel port on the back of the computer (usually LPT1). Note, however, that new computers no longer include a Parallel port. Also, all new dongles are USB. If you are replacing an old computer and currently use a Parallel dongle, contact Eclipse Customer Support to get a USB replacement dongle.

If you are using a USB dongle, then it can be installed in any available USB port.

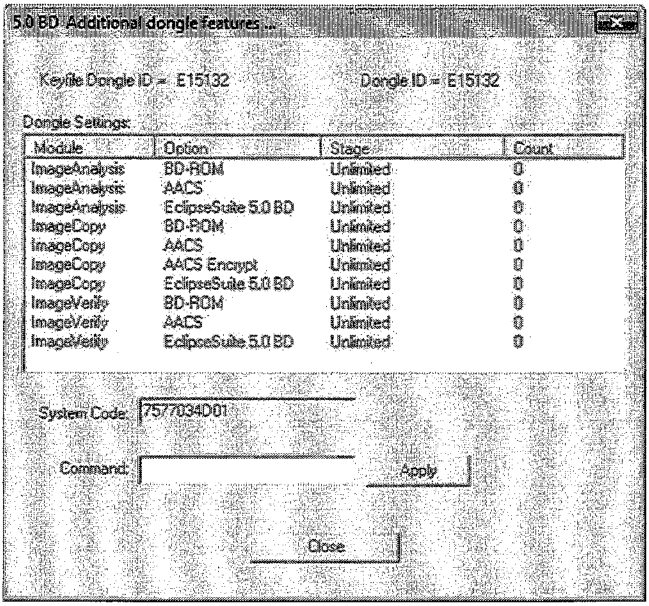
EclipseSuite Software Activation

The EclipseSuite software is protected via a dongle that connects to the parallel or USB port. This dongle must be installed in order for the software to operate. In addition, this software version must be activated through a **Command Code** before it can be used for normal operation. If you are upgrading to EclipseSuite BD 5.0, it is possible that this is already activated. However, it may still need to be unlocked for unlimited operation. If this is a first-time installation of EclipseSuite software, then your system dongle may already be activated.

Determining if EclipseSuite is Already Activated

To determine if EclipseSuite is already activated:

1. Open any of the EclipseSuite programs (ImageAnalysis, ImageCopy or ImageVerify). Click **File | Dongle Password | More** to display the **Additional dongle features** window.



5.0 BD Additional dongle features ...

Keyfile Dongle ID = E15132
Dongle ID = E15132

Dongle Settings:

Module	Option	Stage	Count
ImageAnalysis	BD-ROM	Unlimited	0
ImageAnalysis	AACS	Unlimited	0
ImageAnalysis	EclipseSuite 5.0 BD	Unlimited	0
ImageCopy	BD-ROM	Unlimited	0
ImageCopy	AACS	Unlimited	0
ImageCopy	AACS Encrypt	Unlimited	0
ImageCopy	EclipseSuite 5.0 BD	Unlimited	0
ImageVerify	BD-ROM	Unlimited	0
ImageVerify	AACS	Unlimited	0
ImageVerify	EclipseSuite 5.0 BD	Unlimited	0

System Code: 7577034D01

Command:

Figure 1: Additional dongle features...

The second column shows the options that are activated on the dongle. The Stage column shows the option's current status. The picture above shows that **EclipseSuite 5.0 BD** has been activated for unlimited use.

> **NOTE**
> *Since EclipseSuite 5.0 BD is specific to Blu-ray images, you will likely need activations for the 'BD-ROM' option and possibly 'AACS' and 'AACS Encrypt'. However, if you are upgrading from a previous version, it is likely that only the 'EclipseSuite 5.0 BD' option is required.*

2. If EclipseSuite 5.0 BD is already activated and is set for unlimited use, then you do not need any dongle activations. However, if EclipseSuite 5.0 BD is already activated but it is set for evaluation only (i.e. Evaluation Stage II), then you will need an activation to unlock it for unlimited use.
3. If the EclipseSuite 5.0 BD option is not listed in the **Additional dongle features** window, then this option has not been activated. Make note of the **System Code** and contact Eclipse or an Eclipse Distributor in your region.

> **NOTE**
> *Is you are using a previous version of EclipseSuite to check if EclipseSuite 5.0 BD has been activated then it is possible that the "EclipseSuite 5.0 BD" option may not appear in the list. The reason is that older versions may not recognize newer versions of the EclipseSuite software.*

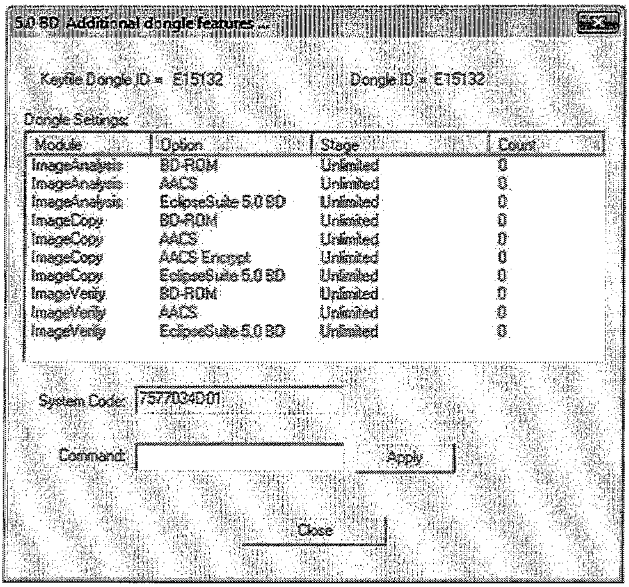
Activating EclipseSuite 5.0 BD

To activate or unlock the EclipseSuite software, you will need to provide Eclipse with a **System Code**. This **System Code** can be obtained from the software once it is installed. Refer to section ***Obtaining a System Code*** for details on how you can get the **System Code**.

You must contact Eclipse Data Technologies Customer Support or your local Eclipse Distributor to request a software activation code. The **System Code** will be required. You can make your request via telephone or email. Once you receive your activation code from Eclipse, follow the procedures below to activate the software.

To activate EclipseSuite:

1. Open any of the EclipseSuite programs (ImageAnalysis, ImageCopy or ImageVerify). Click **File | Dongle Password | More** to display the **Additional dongle features** window.



5.0 BD Additional dongle features ...

Keyfile Dongle ID = E15132 Dongle ID = E15132

Dongle Settings:

Module	Option	Stage	Count
ImageAnalysis	BD-ROM	Unlimited	0
ImageAnalysis	AACS	Unlimited	0
ImageAnalysis	EclipseSuite 5.0 BD	Unlimited	0
ImageCopy	BD-ROM	Unlimited	0
ImageCopy	AACS	Unlimited	0
ImageCopy	AACS Encrypt	Unlimited	0
ImageCopy	EclipseSuite 5.0 BD	Unlimited	0
ImageVerify	BD-ROM	Unlimited	0
ImageVerify	AACS	Unlimited	0
ImageVerify	EclipseSuite 5.0 BD	Unlimited	0

System Code: 7577034D01

Figure 2: Additional dongle features

2. Enter the command code in the **Command** box then click **Apply**. It will take a few seconds to program the new version. You should see a message indicating that activation was successful.
3. When you are prompted to backup the dongle key files. You can backup the keys to the original Key Files Diskette or USB thumb drive, or you can click **Cancel** to continue without backing up the keys.

If you have any questions or problems activating the EclipseSuite software, please contact Eclipse Customer Support or your local distributor.

Eclipse Customer Support
Phone: 925-598-0300
Email: support@eclipsedata.com

This page has been left blank intentionally.

Certificate Management Utility (CMU)

Introduction

The Certificate Management Utility (CMU) is designed to help manage the handling of content certificates required for AACS encryption. It is configured to monitor directories for the presence of AACS images. The CMU will display the AACS encryption status of each BD image and allow the user to perform several AACS post-encryption tasks that are required before an image can be mastered.

CMU Key Features

- **Content Certificate Extraction**

  The CMU allows users to extract the unsigned Content Certificate from images so that they can be submitted to AACS LA for signing. The CMU extracts all of the file(s) required and packages them into a single file in the format defined by AACS LA. Once the file is extracted, users can submit it to AACS LA.

- **Content Certificate Validation**

  The CMU verifies that the signed Content Certificate returned from AACS LA matches the image that the user is trying to sign. It does this using the date and license ID. This is a very important safeguard because AACS filenames are confusing.

- **Application process is done with post encrypted images.**

  By using the CMU there no need to stop ImageCopy in the middle of the encryption process. ImageCopy can finish the encryption and the CMU will apply the certificates later when received from AACS LA.

  CMU allows the user to quickly apply updated MKBs to post-encrypted images without the need to re-encrypt the data. The new image will have freshly encrypted Title Keys, Partial Media Key Block for lead-in, and a Volume ID.

- **Manual or Automation Process**

  Users can configure the CMU to run in manual or automatic modes. In manual mode, every action is driven by the user via the user interface. In automatic mode, the CMU can automatically sign an image as its signed Content Certificates arrives.

  - Scans predefined directories and display all BD image and their AACS status.
  - Export an unsigned certificate with a valid filename.
  - Identifies incoming signed certificates, PGP decrypts and signs the matching image.
  - Manages the use of MKB keys so that key selection is automatic and they don't get re-used.

- **Automatic Updating of Image Checksums**

  When an image is signed, the CMU can be configured to automatically update the image integrity files. The signing process updates files in the image so it is necessary to update the checksums and SHA-1 values.

CMU Requirements

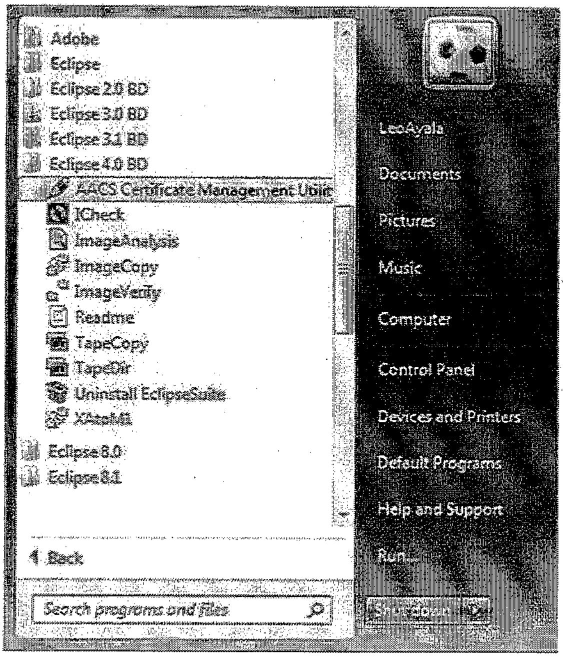
- Complete installation of a Blu-ray supported EclipseSuite software version.

- Required EclipseSuite Dongle activations
- ImageCopy AACS Encryption

Installation

The CMU is part of the EclipseSuite BD software installation package. Therefore, a complete installation of the EclipseSuite BD software is required.

The CMU can be launched from the shortcut that is created during installation or directly from the installation folder.

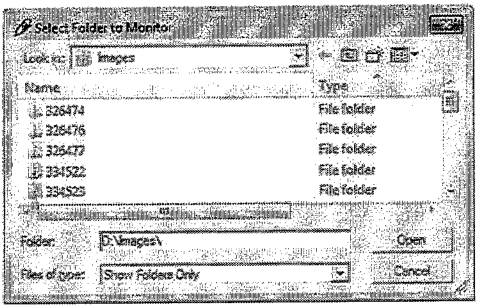

Adobe
Eclipse
Eclipse 2.0 BD
Eclipse 3.0 BD
Eclipse 3.1 BD
Eclipse 4.0 BD
AACS Certificate Management Utilit
ICheck
ImageAnalysis
ImageCopy
ImageVerify
Readme
TapeCopy
TapeDir
Uninstall EclipseSuite
XAtoM
Eclipse 8.0
Eclipse 8.1
Back
Search programs and files
LeoAyala
Documents
Pictures
Music
Computer
Control Panel
Devices and Printers
Default Programs
Help and Support
Run...
Shut down

Configuration

There are a few settings that must be configured depending on whether the CMU will be run in manual or automatic mode.

Monitoring Folder

When the CMU is launched, it first prompts the user to select the folder containing the images that it will monitor.



Select Folder to Monitor

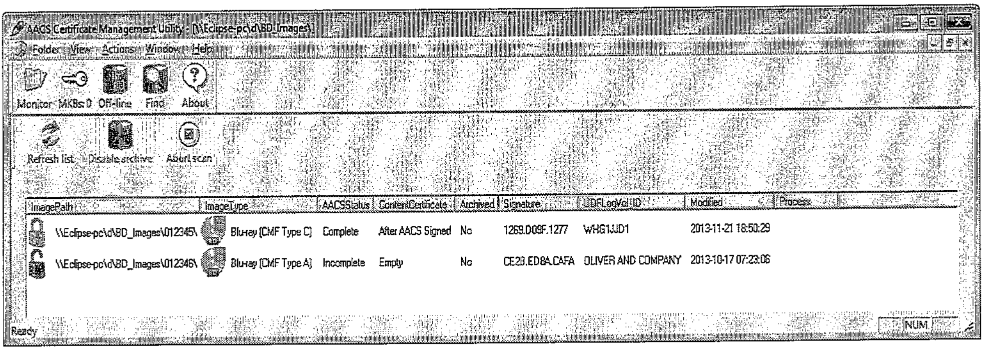
Look in: Images

Name	Type
326474	File folder
326476	File folder
326477	File folder
334522	File folder
334523	File folder

Folder: D:\Images\

Files of type: Show Folders Only

When a folder is selected, the CMU displays the list of BD images in that folder and their properties.



AACS Certificate Management Utility - [\\Eclipse-pc\d\BD_Images\]

ImagePath	ImageType	AACSStatus	ContentCertificate	Archived	Signature	UDFLogVol ID	Modified	Process
\\Eclipse-pc\d\BD_Images\012345\	Blu-ray (CMF Type C)	Complete	After AACS Signed	No	1269.D09F.1277	WHG1JJD1	2013-11-21 18:50:29	
\\Eclipse-pc\d\BD_Images\012346\	Blu-ray (CMF Type A)	Incomplete	Empty	No	CE2B.ED8A.CAFA	OLIVER AND COMPANY	2013-10-17 07:23:06	

Typically there will be a single folder where the images are stored. However, if it is necessary, additional folders can be monitored by clicking on the Monitor button in the toolbar. Additional folders will be listed in separate windows.

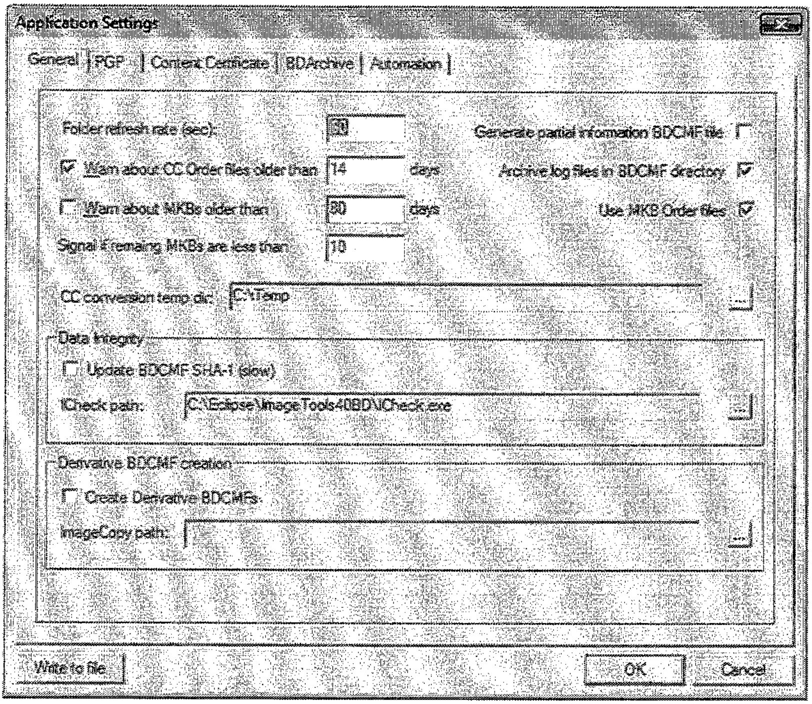
A folder must be selected regardless of whether the CMU is running in manual or automatic mode.

Application Settings

The remainder of the configuration is done via the CMU Application Settings. The Application Settings are divided into different categories each displayed under its own tab window and they are described below.

General Settings

The General settings window is used to configure all miscellaneous settings.



Folder refresh rate (sec): 60

☑ Warn about CC Order files older than 14 days

☐ Warn about MKBs older than 30 days

Signal if remaing MKBs are less than 10

Generate partial information BDCMF file ☐

Archive log files in BDCMF directory ☑

Use MKB Order files ☑

CC conversion temp dir: C:\Temp

Data Integrity

☐ Update BDCMF SHA-1 (slow)

ICheck path: C:\Eclipse\ImageTools40BD\ICheck.exe

Derivative BDCMF creation

☐ Create Derivative BDCMFs

ImageCopy path:

> **NOTE**
> *All settings are stored in the system registry but a copy of the settings can be saved to a file by clicking on* ***Write to file.***

Folder refresh rate (sec)

This setting allows the user to specify the frequency at which the Monitored Folder will be refreshed. The default is 60 seconds.

Note that as more images are added to the folder, the longer it will take the CMU to refresh the whole list. Therefore, as the list grows, make sure that the refresh rate is increased accordingly.

Warn about CC Order files older than 14 days

For security reasons, the AACA LA requires that users check if the order generation date does not match the actual order timeframe.

AACS will process all CC Orders promptly in the order they are received. In the process of signing a Content Certificate, AACS LA will record an order generation timestamp in the order file header. It is assumed that users will sign an image shortly after receiving the CC Order file from AACS LA. When signing an image, the CMU checks the order generation timestamp to the local computer's date/time. If the difference is more than 14 days (default), then a warning message is displayed.

Warn about MKBs older than 80 days

Similar to CC Order files, the AACS LA also requires that users check the order generation date for MKB Order files. However, in the case of MKB Order files, the default number of days is 80. The reason is that MKB Order files can include a maximum of 500 individual MKB so it will take some time before all MKB's are consumed.

Signal if remaining MKBs are less than 10

This option triggers a message to the user when the number of MKBs remaining reaches 10 or less. One MKB is consumed per image during the signing process. Therefore, this option should be set to a value that will give you enough time to place an order with AACS LA for the purchase of additional MKBs.

Generate partial information BDCMF file

This option allows users to create the necessary files for a Type AX image (i.e. Type A with Partial Information). The option creates a folder and places the files in it. The user must take those files along with the original source image to make a Type AX image and return it to the customer. This will allow the customer to send the Type AX image for re-mastering without having to pay for new CC again.

NOTE
Although Type A with Partial Information is an option that is part of the BDCMF specifications, it is recommended that a Type C is returned to the customer instead.

Archive log files in BDCMF directory

Starting with version 1.20, the BDCMF specifications support storing of data related to a BDCMF image to be stored in the file CMF-DOCS.ZIP. In the case of the Eclipse tools, users can store the log files generated throughout the production chain. This option instructs the CMU to store any logs it generates in the CMF-DOCS.ZIP file.

Use MKB Order files

When signing an image, the CMU can search or prompt for an individual MKB or for an MKB Order file. An MKB Order file consists of up to 500 individual MKBs in a single file. When this option is selected, the CMU will default to expect an MKB Order file, although users can still select an individual MKB. When an MKB Order file is copied to the Media Key Block Order directory, the CMU automatically extracts all of the individual MKBs.

If this option is not selected, it is expected that the user will extract the individual MKBs from the MKB Order file.

CC conversion temp dir

This option is no longer used.

Data Integrity

When signing an image, the Content Certificate and possibly other files will be updated on the image. The updating of these files requires updating of the file checksums and SHA-1. To update these, the CMU requires knowing where ICheck is located.

ICheck path

This specifies the path to the ICHECK application that is used to update file checksums. Click on the button at the right of to select the ICHECK application.

NOTE
The CMU and ICHECK are utilities that are included with the EclipseSuite BD software. When upgrading to a new version of the CMU, it is recommended that you also update the path to use the new version of ICHECK.

Update BDCMF SHA-1 (slow)

Similar to Eclipse file checksums, the BDCMF specifications support a SHA-1 for the BDCMF.CMF file only. Users can optionally choose to update this checksum. However, to calculate, the whole image needs to be analyzed, which may take some time to complete. Therefore, this option is not selected by default. Note also that when the image is converted from a Type A to a Type B, ImageCopy automatically removes the SHA-1 if it exists. The reason is that to calculate, a second pass would have to be made.

NOTE
Although ImageCopy removes the SHA-1 value, the BDCMF.CMF file is still protected with Eclipse's checksum.

Derivative BDCMF creation

Some studios may require different versions of a Blu-ray Video, for example, a rental vs. retail version. While studios can author two different versions of the same image, this would add additional cost since it would require the CCs to be submitted for each image. This option allows users to create two different versions of the same image using the same CCs. The CMU does this by making a copy of the Type B image and signing both using the same CC returned from AACS LA.

Create Derivative BDCMFs

This enables the option to create two version of the same image.

ImageCopy path

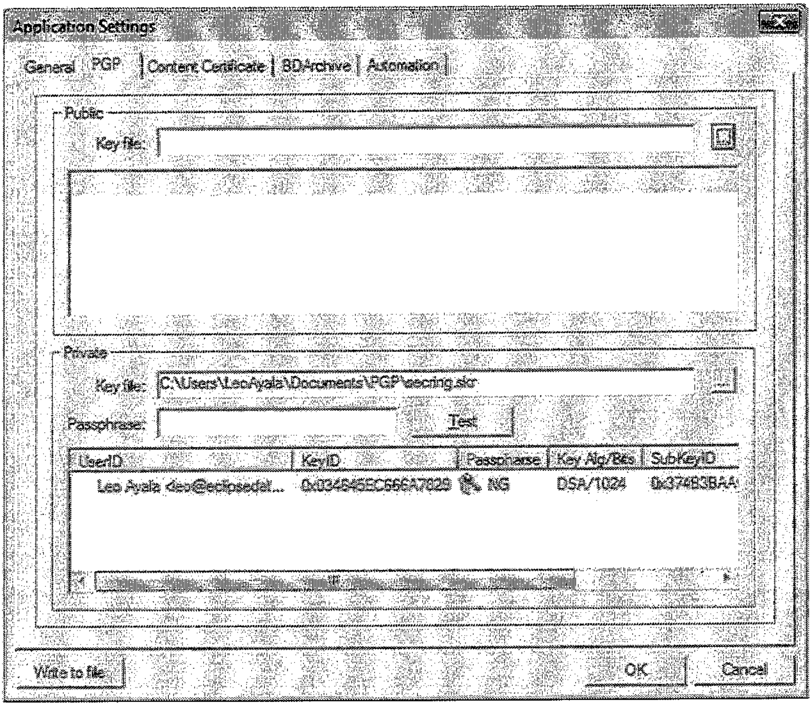
Since it is ImageCopy that actually creates the different images, the CMU requires to know the path to ImageCopy. Click on the button at the right to select ImageCopy.

NOTE
The CMU is a utility that is included with the EclipseSuite BD software. When upgrading to a new version of the CMU, it is recommended that you also update this path to use the new version of ImageCopy.

PGP

The PGP tab appears only if PGP is installed on the local computer. The files submitted to AACS LA and the ones returned from AACS LA are PGP-encrypted. If PGP is not installed, then users must encrypt/decrypt them before they can be used by the CMU. With PGP installed, the CMU can automate the process without user intervention.

Since users will exchange PGP-encrypted files, it is required that customers exchange their PGP Public Keys. Refer to section ***PGP Setup*** for more details.



Key file:

Key file: C:\Users\LeoAyala\Documents\PGP\secring.skr

Passphrase:

UserID	KeyID	Passpharse	Key Alg/Bits	SubKeyID
Leo Ayala <leo@eclipsedat...	0x034545EC666A7829	NG	DSA/1024	0x37483BAA

Public Key File

This option is currently not used.

Private Key File & Passphrase

The Private Key is used to encrypt the unsigned CC Order files before they are sent to AACS LA. It is also used to decrypt the signed CC Order file and MKB Order files that are received from AACS LA.

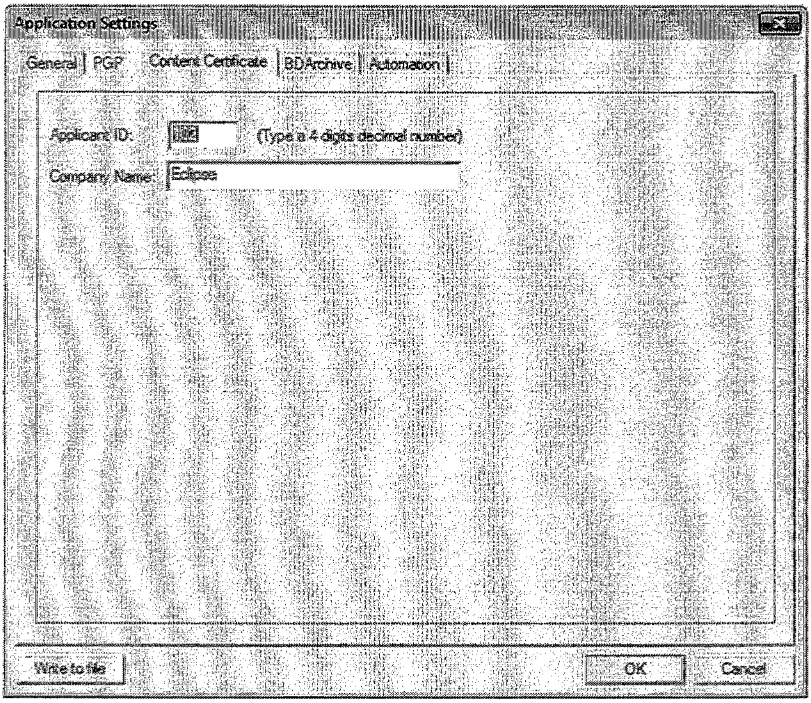
To use the Private Key, the CMU requires that the passphrase that was set when the Private Key was created. For security reasons, the passphrase is not saved by the CMU so it must be entered every time the CMU. When the CMU is first launched, the Passphrase column will show NG, indicating that the passphrase has not been entered. The CMU cannot encrypt or decrypt files until the correct passphrase has been entered. Once the correct passphrase has been entered, the Passphrase column will show OK.

Refer to ***PGP Setup*** for more information.

Content Certificate

The Content Certificate settings are used to specify customer specific information for the generation of the file that is submitted to AACS LA for signing.

AACS LA requires that the CCs that are submitted to them be in a specific filename format that includes the customer's Applicant ID and company name. When extracting the CCs from an image, the CMU will name the filename using these values.


Application Settings
General
PGP
Content Certificate
BDArchive
Automation
Write to file
OK
Cancel

Applicant ID: [illegible] (Type a 4 digits decimal number)

Company Name: Eclipse

Applicant ID

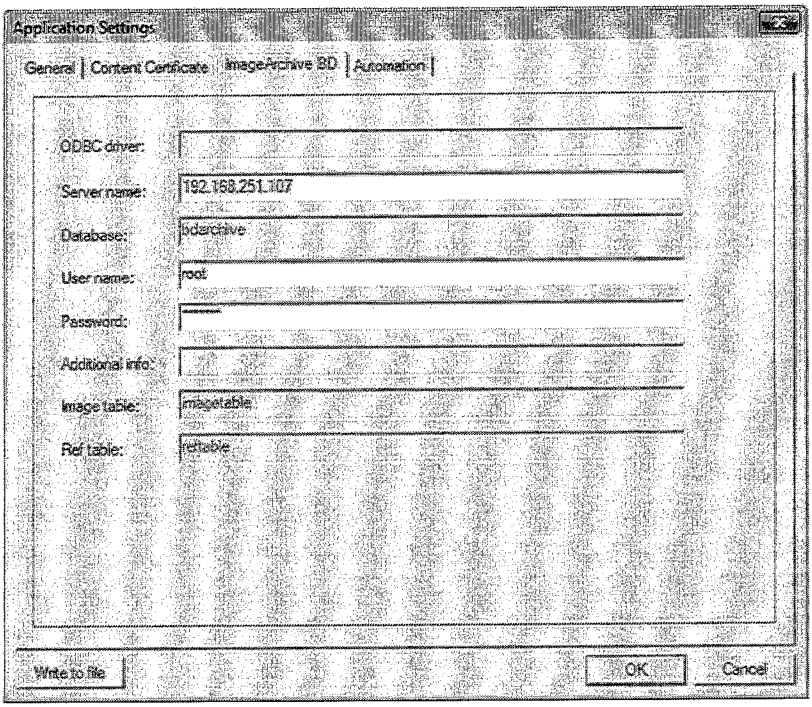
The Applicant ID is a unique ID identifying each AACS licensed customer. This ID is issued by AACS LA.

Company Name

This field must be set to the company name as it was specified in the AACS license agreement.

ImageArchive BD

The ImageArchive BD settings are used to specify the connection information to the computer that is hosting the ImageArchive BD Archive database. Refer to section ***ImageArchive BD Setup*** for more information on the configuration of this option.


Application Settings
General
Content Certificate
ImageArchive BD
Automation
Write to file
OK
Cancel

ODBC driver:
Server name: 192.168.251.107
Database: bdarchive
User name: root
Password:
Additional info:
Image table: imagetable
Ref table: reftable

ODBC driver

This option is currently not used.

Server name

This field must be set to the IP address or computer name that is hosting the BD Archive database.

Database

This field must be set to the name of the database, which is always **bdarchive**.

User name

This field must be set to **root**.

Password

This field must be set to the password assigned to the bdarchive database.

Additional Info

This field is currently not used.

Image table

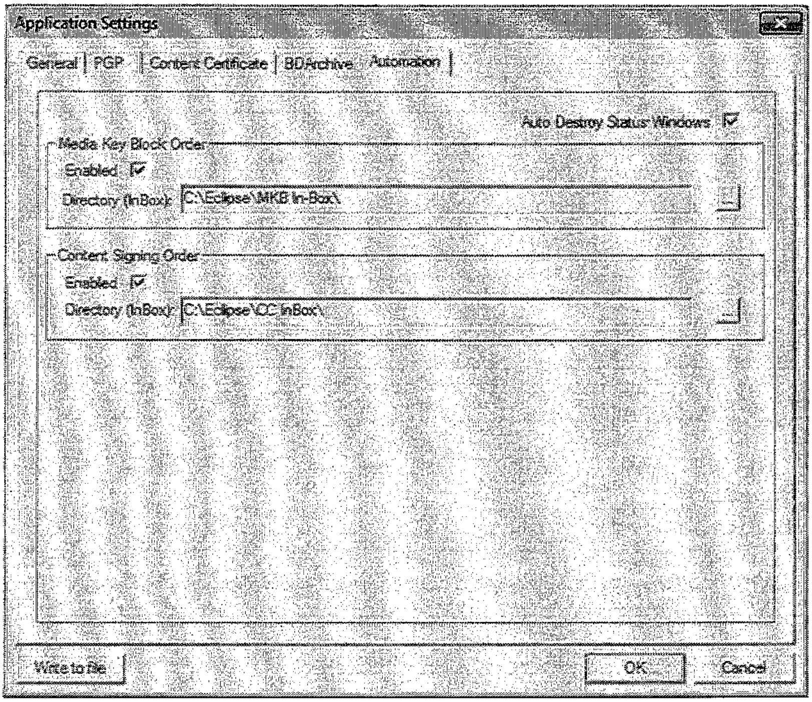
This field must be set to the table in the bdarchive database where the information is to be stored. The default table name is 'imagetable'.

Ref table

This field must be set to the reference table in the bdarchive database. The default reference table name is 'reftable'.

Automation

The Automation settings are used to configure the CMU for either automation or manual mode. In automation mode, the CMU can automatically process MKB Order files. It can also be configured to automatically sign images when a matching CC Order file arrives.



Auto Destroy Status Windows ☑

Media Key Block Order
Enabled ☑
Directory (InBox): C:\Eclipse\MKB In-Box\

Content Signing Order
Enabled ☑
Directory (InBox): C:\Eclipse\CC InBox\

Auto Destroy Status Window

This option automatically closes any status window that appears when an action is being performed on an image. For example, in the process of signing and image, a status window will appear detailing all tasks that are being performed. If this option is selected, the window will be closed automatically when the task is complete. If the option is not selected, the window will remain open until the user closes it manually.

Note that the CMU saves a log in the image directory of all actions performed on an image.

Media Key Block Order

MKBs are purchased from AACS LA in quantities of up to 500. Regardless of the quantity, the MKBs are packaged into a single MKB Order file. A single MKB is consumed per image when the image is signed by the CMU. However, before any MKBs can be used, they must be unpacked from the MK Order file.

Enabling this option allows the CMU to automatically unpack MKB Order files in the specified directory to the individual MKBs.

Enable

This option enables automatic processing of MKB Order files.

Directory (InBox)

This option sets the path that the CMU will monitor for new MKB Order files and where the individual MKBs will be extracted to.

The naming convention for the individual MKB will be based on the filename of the MKB Order file. Normally the MKB Order filename will include a timestamp. The individual MKBs will have the same timestamp with a 4-digit sequential unique number and an FMT extension. Example: **110719_1324:15_0001.FMT**.

Content Signing Order

A Content Singing Order file includes a single Signed Content Certificate returned from AACS LA. Enabling this option allows the CMU to automatically sign the matching image.

Enable

This option enables automatic processing of CC Order files.

Directory (InBox)

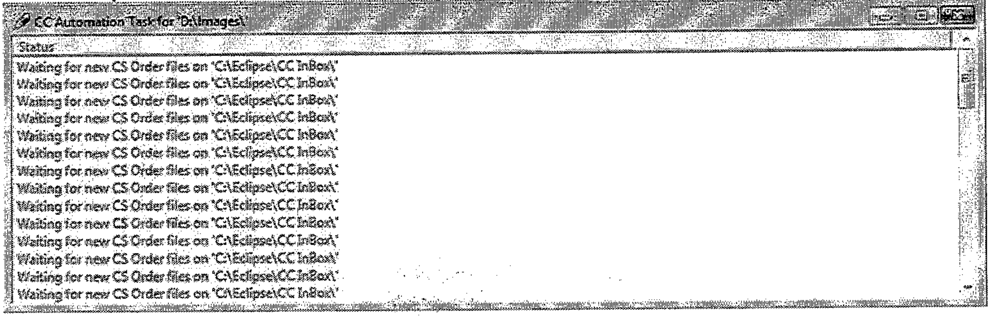
This option sets the path that the CMU will monitor for incoming CC Order files. If this option is enabled, the CMU will automatically sign the image that the CC Order file matches.

> **NOTE**
> *Since the CC Order file is PGP-encrypted when it is returned from AACS LA, it is required that PGP be installed on the local computer in order for this option to work in automatic mode.*

Monitor Folders for CC and MKB Order Files

When enabling automation, a separate monitor window will appear for the Content Signing Order Directory and another for the Media Key Block Order Directory.

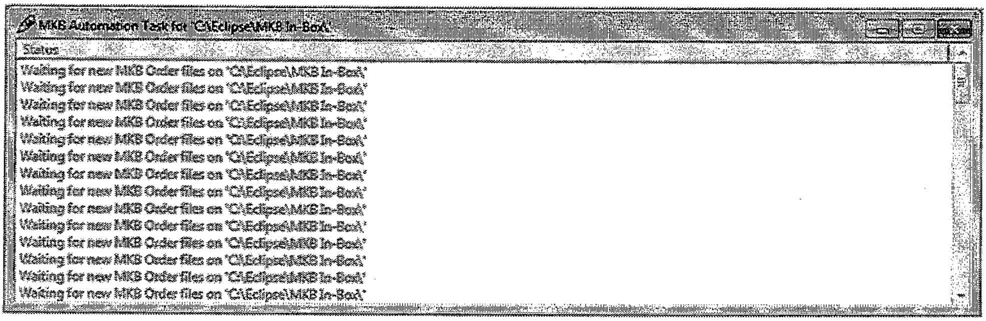
The CC Order monitor window will monitor and log any activity when the user copies a CC Order file into this directory. When one is detected, the CMU will automatically search for its matching image and sign it.



```
Waiting for new CS Order files on 'C:\Eclipse\CC InBox\'
Waiting for new CS Order files on 'C:\Eclipse\CC InBox\'
Waiting for new CS Order files on 'C:\Eclipse\CC InBox\'
Waiting for new CS Order files on 'C:\Eclipse\CC InBox\'
Waiting for new CS Order files on 'C:\Eclipse\CC InBox\'
Waiting for new CS Order files on 'C:\Eclipse\CC InBox\'
Waiting for new CS Order files on 'C:\Eclipse\CC InBox\'
Waiting for new CS Order files on 'C:\Eclipse\CC InBox\'
Waiting for new CS Order files on 'C:\Eclipse\CC InBox\'
Waiting for new CS Order files on 'C:\Eclipse\CC InBox\'
Waiting for new CS Order files on 'C:\Eclipse\CC InBox\'
Waiting for new CS Order files on 'C:\Eclipse\CC InBox\'
Waiting for new CS Order files on 'C:\Eclipse\CC InBox\'
Waiting for new CS Order files on 'C:\Eclipse\CC InBox\'
```

The MKB Order monitor window will monitor and log any activity when the user copies an MKB Order file into this directory. When one is detected, the CMU will automatically extract the individual MKB files and remove the original MKB file. The naming convention for the individual MKB files is as follows:

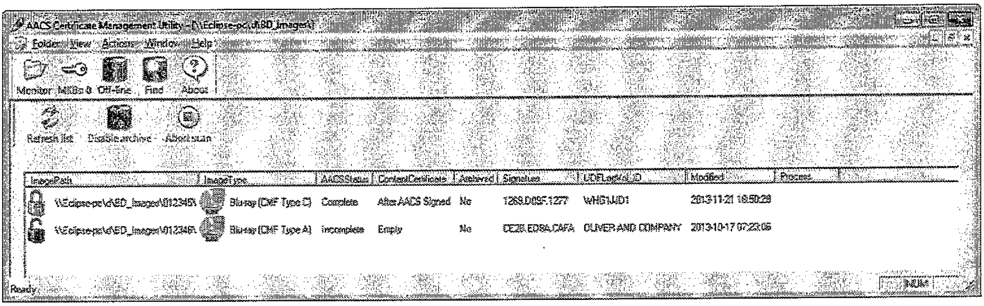
123123123_3412312_0123.fmt
The MKB Order monitor window will also log any activity when an MKB is used for signing an image.



```
Waiting for new MKB Order files on 'C:\Eclipse\MKB In-Box\'
Waiting for new MKB Order files on 'C:\Eclipse\MKB In-Box\'
Waiting for new MKB Order files on 'C:\Eclipse\MKB In-Box\'
Waiting for new MKB Order files on 'C:\Eclipse\MKB In-Box\'
Waiting for new MKB Order files on 'C:\Eclipse\MKB In-Box\'
Waiting for new MKB Order files on 'C:\Eclipse\MKB In-Box\'
Waiting for new MKB Order files on 'C:\Eclipse\MKB In-Box\'
Waiting for new MKB Order files on 'C:\Eclipse\MKB In-Box\'
Waiting for new MKB Order files on 'C:\Eclipse\MKB In-Box\'
Waiting for new MKB Order files on 'C:\Eclipse\MKB In-Box\'
Waiting for new MKB Order files on 'C:\Eclipse\MKB In-Box\'
Waiting for new MKB Order files on 'C:\Eclipse\MKB In-Box\'
Waiting for new MKB Order files on 'C:\Eclipse\MKB In-Box\'
Waiting for new MKB Order files on 'C:\Eclipse\MKB In-Box\'
```

CMU Features

This section describes the CMU features.



AACS Certificate Management Utility - [\\Eclipse-pc\d\BD_Images\]
Folder View Actions Window Help
Monitor
MKBs 0
Off-line
Find
About
Refresh list
Disable archive
Abort scan
Ready
NUM

ImagePath	ImageType	AACSStatus	ContentCertificate	Archived	Signature	UDFLogVol_ID	Modified	Process
\\Eclipse-pc\d\BD_Images\012345\	Blu-ray (CMF Type C)	Complete	After AACS Signed	No	1269.D09F.1277	WHG1JJD1	2013-11-21 18:50:28	
\\Eclipse-pc\d\BD_Images\012346\	Blu-ray (CMF Type A)	Incomplete	Empty	No	CE2B.ED8A.CAFA	OLIVER AND COMPANY	2013-10-17 07:23:06	

CMU Menu

The menu bar includes five menu items that users can use to perform any action on any image. Each menu item is described below.

Folder

The Folder menu allows users to select a folder to monitor, close a currently opened folder and its associated windows or to exit the CMU application. Users can also select a folder monitor by clicking on the folder icon in the toolbar.

View

This menu allows users to show/hide the toolbar, status bar and the CMU tasks windows. For every folder that is being monitored, there is a task window that will show the monitor tasks being performed. If automation is turned on, a second window will appear showing the CC automation tasks.

The View menu includes the item 'View CC Order File', which allows users to view Order File details. This helps users match the order file to the right image when working in manual operation.

Actions

This menu allows the user to perform actions on an image. The actions available depend on the AACS status of the image. The 'Change settings' menu item also allows the user to configure the CMU.

Window

The Window menu provides options to organize the windows that are open in the CMU and to switch between them.

Help

The Help menu allows users to access the online help information that is available in this manual.

CMU Toolbar

The toolbar provides quick access to the most common actions.

Monitor

The Monitor toolbar button is used to select an image folder to monitor. Typically a single folder will be monitored but users can select more than one.

The same action can be achieved via the **Folder | Monitor** menu item.

MKBs:0

The MKBs toolbar button shows the available KMBs in the folder specified in the Automation configuration settings.

The same action can be achieved via the **Actions | Show available MKBs** menu item.

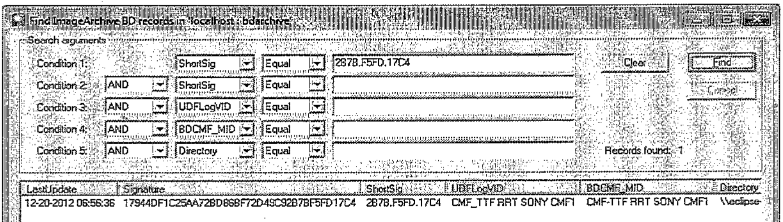
Off-line

The ImageArchive BD button shows the database connection status. When the CMU is connected to the database server it will show Online. Otherwise, it will show Off-line. Clicking on it will test the connection.

The same action can be achieved via the **Actions | Test ImageArchive BD Connection** menu item.

Find

The **Find archive records** button is used to locate database records. While the CMU displays a column indicating whether or not an image has been archived, it may be time consuming to confirm by manually scrolling through the image list if the list is too long. Instead, users can click the Find button and specify the image criteria and the CMU will search the database to see if the image has been archived.


Find ImageArchive BD records in 'localhost : bdarchive'

Search arguments

Condition 1: ShortSig Equal 2878.F5FD.17C4
Condition 2: AND ShortSig Equal
Condition 3: AND UDFLogVID Equal
Condition 4: AND BDCMF_MID Equal
Condition 5: AND Directory Equal

Records found: 1

LastUpdate	Signature	ShortSig	UDFLogVID	BDCMF_MID	Directory
12-20-2012 06:56:36	17944DF1C25AA72BD86BF72D49C92B7BF5FD17C4	2878.F5FD.17C4	CMF_TTF RRT SONY CMF1	CMF-TTF RRT SONY CMF1	\\eclipse-

Clicking on the Find button has the same effect as clicking on the menu item **Actions | Find archive records.**

Note that this action only checks whether the image you searched for has been archived to the

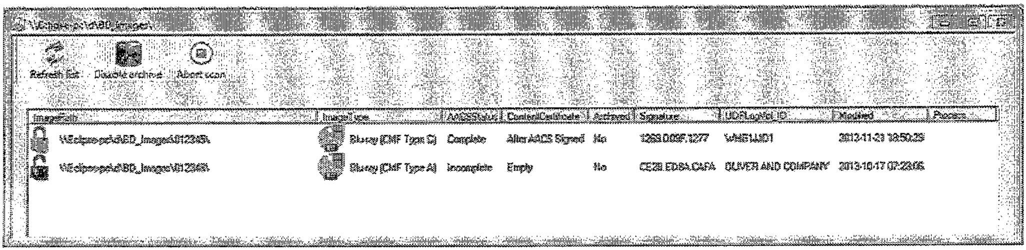
ImageArchive BD database. It does not locate an image within the CMU image list.

About

The About toolbar button displays the version of the CMU. You can also view the version information by clicking **Help | About AACSTool**.

Monitor Folder

For every folder that the CMU is monitoring, it displays a window with a list of images found in the folder. The list is used to display AACS status information.



Each Monitor Folder window includes a toolbar with the following three buttons.

The **Refresh** button forces the CMU to refresh the monitored image list. The CMU is set to automatically refresh every 60 seconds. However, be aware that the more images exist, the longer it may take the CMU to refresh the list. The image list will be grayed when the list is being updated. If it remains grayed out for too long, then it means that there are too many images in the list and the CMU cannot finish refreshing the list at the interval specified in the configuration settings. A faster computer and/or more memory can speed up the refresh process.

The same action can be achieved via the **Actions | Refresh image list** menu item.

The **Disable archive** button is used to disable the ImageArchive BD operation. This may be useful when you need to sign an image right away but archive operations may be taking too long to complete.

The Abort scan button is used to abort the scanning of images that occurs as at preconfigured intervals. This is useful for users who maintain a lot of images. The longer the list, the longer it will take the CMU to traverse through the list. If the CMU is taking a long time scanning for images and you have an image to sign, clicking this button will abort the scan.

Each Monitored Folder includes image list. The list includes columns to describe the image and its AACS and Archive status.

Image Path

The image path specifies the folder where the image is located. A green lock icon is used to identify images that are ready for mastering (Type C) while a red lock icon is used to identify images that are not yet ready for mastering (Type A, B or other).

Image Type

The image type specifies the AACS process status of the image (i.e. BDCMF Type). The common BDCMF Type are Types A through C. For a complete list and description, refer to ***Basic Types of BDCMF***.

AACS Status

The AACS status column is related to the Image Type column as it specifies the AACS status of an image. Image Types A and B are at an intermediate state and are considered **Incomplete.** Type C images are ready for mastering so they are considered **Complete.**

Content Certificate

This column is also linked to the Image Type and AACS Status columns. It specifies the signed status of the image Content Certificate. A Type A image will show **Empty** since it hasn't been processed yet. A Type B image will show **Before AACS Signed** since it has been encrypted but not signed yet. A Type C will show **After AACS Signed** once the image is signed and becomes ready for mastering.

Archived

The Archived column specifies if an image has been archived to the ImageArchive BD database. If the ImageArchive BD option is setup, the archive process happens automatically when an image is converted to Type C.

Signature

This column displays the image's short signature.

UDFLogVol_ID

This column shows the image's UDF Volume ID, which is usually the title of the Blu-ray Video.

Modified

This column displays the last modified date of the image.

Process

This column will display information about the current process being performed on an image.

Monitor Tasks

For each monitored folder, the CMU also opens a window that maintains a log of all tasks being performed on the monitored folder. By default, the information in this log will be overwritten every time the CMU refreshes the image list.

Common CMU Tasks

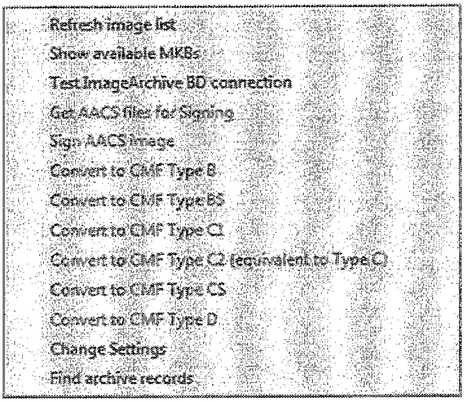
This section describes the common tasks available in the CMU.

Extracting the CC for Signing

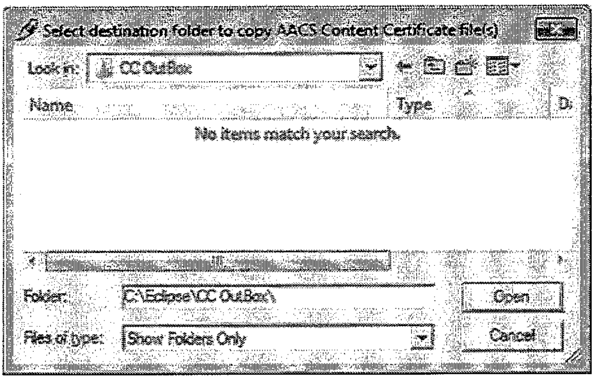
When an image has been encrypted (Type A to Type B conversion), the CCs are ready to be extracted and submitted to AACS LA for signing.

To extract the CC:

1. Right-click on the Type B image as it appears in the CMU monitored folder image list and click on **Get AACS files for Signing.**


Refresh image list
Show available MKBs
Test ImageArchive BD connection
Get AACS files for Signing
Sign AACS image
Convert to CMF Type B
Convert to CMF Type BS
Convert to CMF Type C1
Convert to CMF Type C2 (equivalent to Type C)
Convert to CMF Type CS
Convert to CMF Type D
Change Settings
Find archive records

2. You will be prompted to select a folder where the CMU should extract the unsigned CC.


Select destination folder to copy AACS Content Certificate file(s)

Look in: CC OutBox

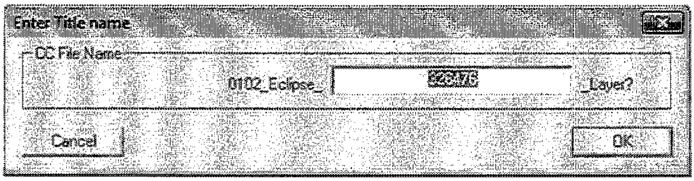
No items match your search.

Folder: C:\Eclipse\CC OutBox\

Files of type: Show Folders Only

Name
Type
D
Open
Cancel

3. AACS LA requires a specific naming convention for the unsigned CCs submitted for signing. After specifying the folder where the CC will be extracted to, you will be prompted for the CC filename.



0102_Eclipse_ [illegible] _Layer?

The filename of the extracted file will be based on the Applicant ID, Company Name that is configured in the CMU **Application Settings (Action | Change Settings)**, as well as the title and number of layers of the image. The CMU will automatically create the file with the pre-configured settings but will allow the user to enter the title of the video.

4. After specifying the proper title, click OK and a window will appear showing the status of the CC extraction. Note, however, that it is possible that this action may occur very fast and you may not be able to see this window. To keep the extraction status window open, disable the option **Auto Destroy Status Window** in the Automation Application Settings (Actions | Change Settings | Automation).

5. AACS LA requires that all unsigned certificates be PGP-encrypted. If PGP is installed and setup in the CMU, the extracted files will be automatically encrypted. If you do not have PGP setup to work with the CMU, then you must PGP-encrypt the unsigned CC Order file manually. Refer to ***PGP Setup*** for more information on PGP.

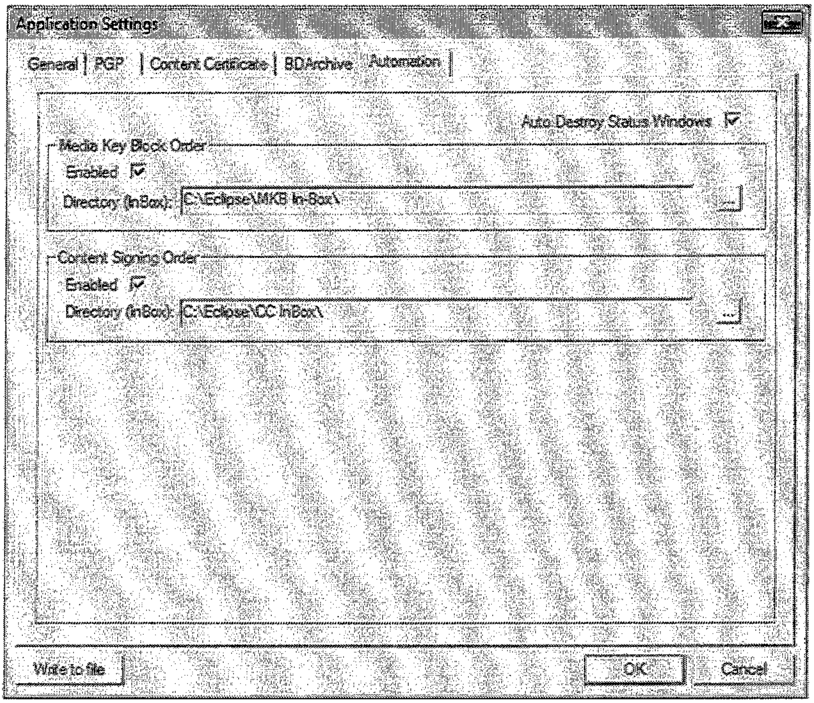
6. After the unsigned CCs are PGP-encrypted they are ready to be submitted to AACS LA for signing.

Signing an Image

Signing an image involves applying the Singed CC Order file back on to the image. When working in manual mode, it is important that users match the Signed CC Order file to the correct image. When working in automation mode, the CMU will automatically match both.

Automatic Mode

Automatic mode can be enabled in the **Automation Application Settings** (Actions | Change Settings | Automation). Additionally, you must specify the folders for MKBs and Signed CC Order files.



Auto Destroy Status Windows ☑

Media Key Block Order
Enabled ☑
Directory (InBox): C:\Eclipse\MKB In-Box\

Content Signing Order
Enabled ☑
Directory (InBox): C:\Eclipse\CC InBox\

The Media Key Block Order In-Box Directory specifies the folder where the CMU can find an MKB. Since an MKB Order file may consist of up to 500 individual MKBs, if the CMU finds an MKB Order file, it automatically extracts the individual MKBs. The CMU will also decrypt the MKB Order file if necessary and if PGP has been setup. Only one MKB file is consumed per image.

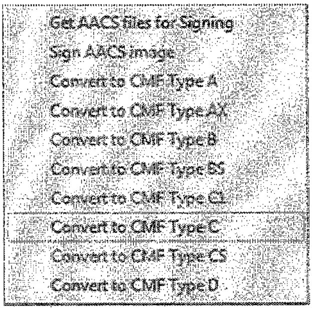
The Content Signing Order In-Box Directory specifies where the CMU can find the Signed CC Order files.

The CMU will automatically decrypt the CC Order file if necessary and if PGP has been setup. The CMU automatically matches the CC Order file to the correct image and signs it.

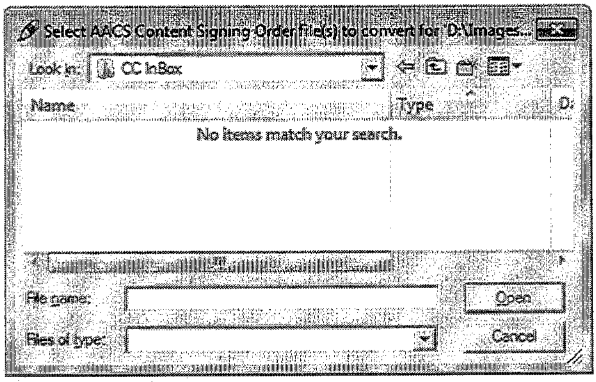
Manual Mode

To sign an image in manual mode:

1. Right-click on the Type B image to be signed and a popup menu with the available actions will appear.


Get AACS files for Signing
Sign AACS image
Convert to CMF Type A
Convert to CMF Type AX
Convert to CMF Type B
Convert to CMF Type BS
Convert to CMF Type C1
Convert to CMF Type C
Convert to CMF Type CS
Convert to CMF Type D

2. From the popup menu select **Convert to CMF Type C** and you will be prompted to select the CC Order file for this image.


Select AACS Content Signing Order file(s) to convert for 'D:\Images...
Look in:
CC InBox
Name
Type
D:
No items match your search.
File name:
Files of type:
Open
Cancel

3. Select the CC Order file then click Open. This will cause the CMU to update the CC and possibly other files back onto the image. This process is referred to as 'Signing'.

4. During the signing process, a status window will appear showing details of every action. If the signing process occurs to fast, then it may be possible that you may not be able to see the details of this status window. You can disable the option **Auto Destroy Status Window** in the Automation Application Settings (Actions | Change Settings | Automation), which will cause the status window to remain open.

5. When the signing process is complete, AACS status of the image will change to a Type C, indicating that it is ready for mastering.

NOTE

If there are any errors during the signing process it usually indicates that you may be signing the image with a CC Order file from a different image. Make sure that you match the correct CC Order file to the image. When you first extract the CC from the image for signing, the Title that you specify in the filename should be something that can uniquely identify each image.

Updating File Checksums

The signing process, the image is updated with the signed CC (and other) files. This means that at the end o this process, the image checksums must be updated. If you have setup ICheck in the Application Settings, the CMU automatically launches ICHECK in the background to update the file checksums.

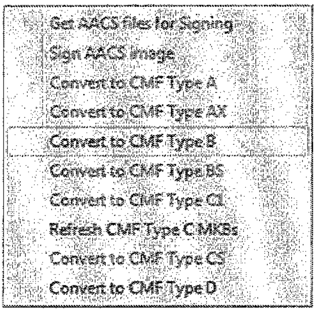
Converting a Type C Image Back to a Type B

There may be cases in which it may be necessary to convert a Type C image back into a Type B. This should not happen often. However, if an image is signed with the wrong CC, then this procedure is necessary.

> **NOTE**
> *This should not be necessary when running in automation mode since the CMU ensures that a Signed CC matches the image. If you are running in automation mode and the image fails after signing, contact Eclipse Customer Support for assistance.*

To convert a Type C to a Type B:

1. Right-click on the Type C image and select **Convert CMF to Type B** from the popup menu.


Get AACS files for Signing
Sign AACS image
Convert to CMF Type A
Convert to CMF Type AX
Convert to CMF Type B
Convert to CMF Type BS
Convert to CMF Type CI
Refresh CMF Type C MKBs
Convert to CMF Type CS
Convert to CMF Type D

2. The action above will cause the CMU to clear the CC in the image back into an unsigned state (i.e. Type B). If ICheck is setup, that image checksums will also be updated.

3. Refer to Signing an Image for details on how to re-sign the image (i.e. convert to Type C).

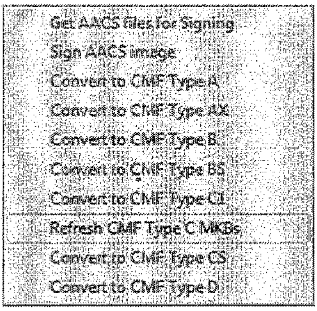
> **NOTE**
> *Every time an image is signed, the Signed CC Order files are deleted after the signing process is complete. If an image is converted back to a Type B, you must have the Signed CC Order file available so that it can be signed again.*

Updating MKBs for a Type C Image

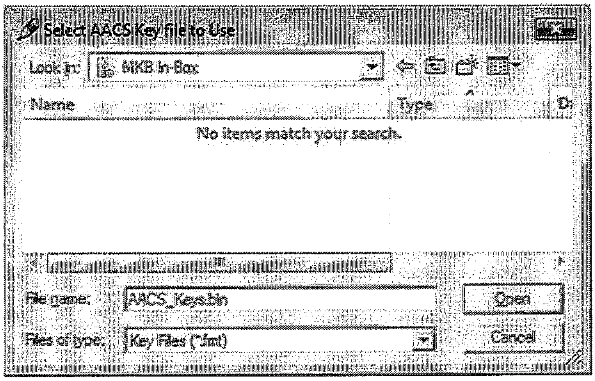
There may be cases when a replicator may need to send a Type C image to another replicator. Similarly, a customer who has a Type C image may send the image to more than one replicator for replication. The Type C image includes an MKB that is unique to the replicator that originally signed the image. If the image is sent to a different replicator, the BDCMF specifications recommend that a replicator receiving a Type C image refresh the MKB with one of their own. This process can be achieved with the CMU.

To refresh the MKB:

1. Right-click on the Type C image and select **Refresh CMF Type C MKBs** from the popup menu.


Get AACS files for Signing
Sign AACS image
Convert to CMF Type A
Convert to CMF Type AX
Convert to CMF Type B
Convert to CMF Type BS
Convert to CMF Type C1
Refresh CMF Type C MKBs
Convert to CMF Type CS
Convert to CMF Type D

2. The action above will cause the CMU to clear the signed CC from the Type C image and converting it back to a Type B. Then, it will prompt for the new MKB.


Select AACS Key file to Use
Look in:
MKB In-Box
Name
Type
D
No items match your search.
Open
Cancel

File name: AACS_Keys.bin

Files of type: Key Files (*.fmt)

3. Select an MKB (or FMT) file and click Open to apply the selected MKB. Although you may not see any change in the AACS status of the image, this action will refresh the image MKB with one of your own.

CMU Logs

The CMU maintains a log file for every monitored folder. The log file is stored in the monitored folder and has a CMU extension. For every action that is performed on an image, the CMU will create another log in the image directory. The filename for every action depends on the action itself. For example, after a conversion from a Type B to a Type C, the log file created will be **B_TO_C_yymmdd_hhmmss.cmu**. The Date/Time will be the date and time when the action took place.

Similarly, when the unsigned CC is extracted from an image, the log CCOut.cmu is created.

The information in these logs help diagnose problems that may occur during an operation. When log files are requested for a problem that occurred in the CMU, these logs should always be included.

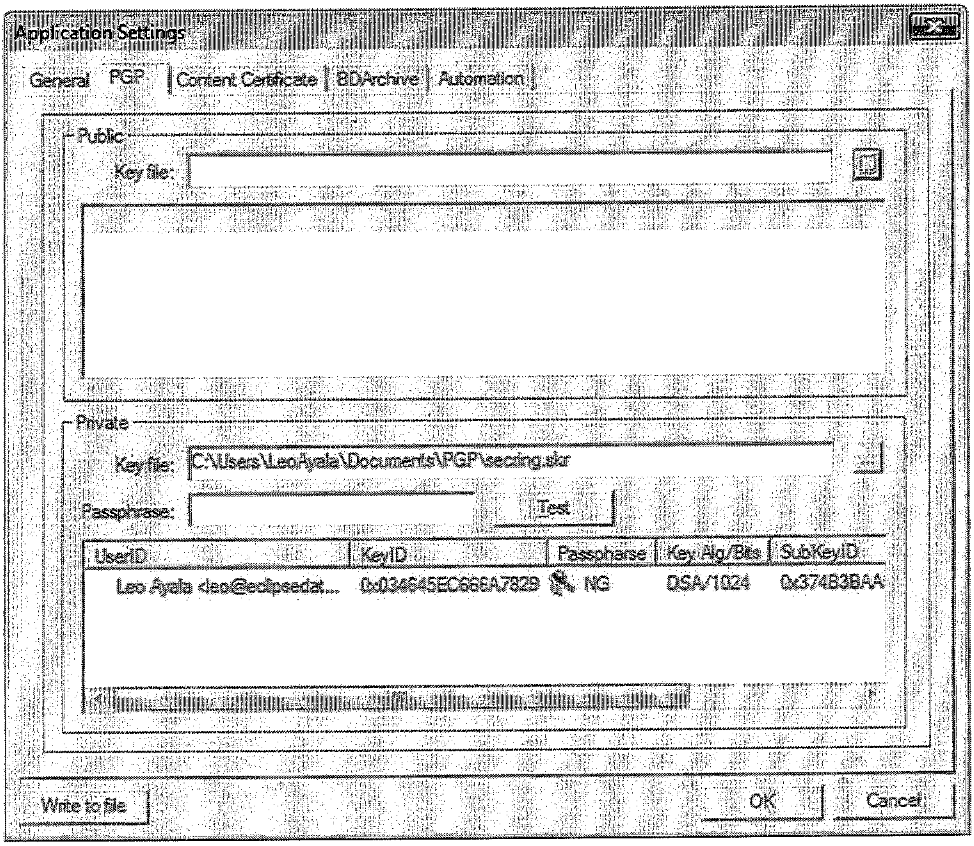
The logs are text files that can be opened with any text editor. Although the content of these logs was intended for Eclipse Support engineers when debugging problems, you should be able to interpret most information. Keep in mind that each action on an image generates a different log file. Therefore, knowing which log file you are looking at should help you follow the tasks that were performed and determine whether it was successful or if any problems occurred.

This page has been left blank intentionally.

PGP Setup

For security reasons, the files exchanged with AACS LA must be encrypted using PGP. This section describes the PGP setup within the CMU. The general installation and configuration of PGP is beyond the scope of this document. Refer to the PGP documentation for installation and configuration details.

During the PGP setup, users are asked to create a matching Private and Public key pair. The private key remains in the user's local computer and the public key is shared with other PGP users who they wish to exchange encrypted files with. In the case of AACS, users will be exchanging encrypted files with AACS LA. Therefore, users must share their public keys with AACS LA. In return, AACS LA will send their public key which users can import into their PGP.


Application Settings
General
PGP
Content Certificate
BDArchive
Automation
Public
Key file:
Private
Test
Write to file
OK
Cancel

Key file: C:\Users\LeoAyala\Documents\PGP\secring.skr

Passphrase:

UserID	KeyID	Passpharse	Key Alg/Bits	SubKeyID
Leo Ayala <leo@eclipsedat...	0x034645EC666A7829	NG	DSA/1024	0x374B3BAA

This page has been left blank intentionally.

Operation

Manual Operation

The CMU will display valid Blu-ray images. Each image will be identified by its source path and image type. The CMU will also display the AACS Status and Content Certificate Status of the image, as well as a modification date. It is essential that the CMU operator understand the various states an image type can be in.

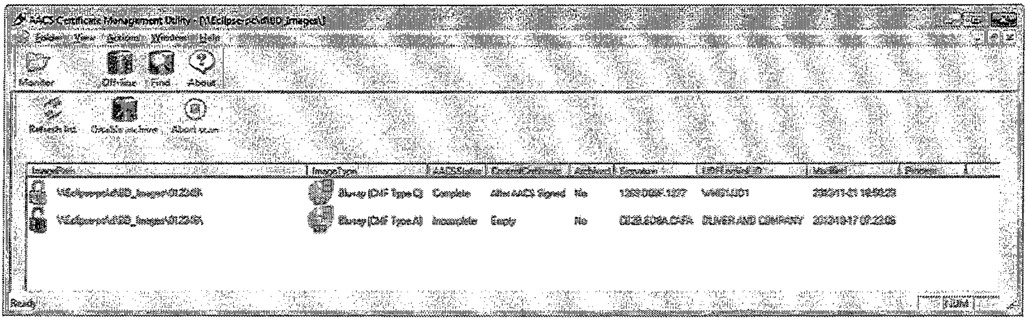


Figure 3: CMU Main Window

Blu-ray (CMF Type A): Incomplete Empty: This is the BDCMF Type received from the authoring facility. This image will need to be encrypted to a Type B using ImageCopy before the CMU can export a content certificate.

Blu-ray (CMF Type B): Incomplete Before AACS Signed: This image has been encrypted by ImageCopy and is ready for two operations:

- Get AACS Files for Signing:
- Convert to Type C:

Extracting AACS Files for Signing

1. Right click on your Type B image and select ***Get AACS Files for Signing.***

   This option will allow the user to create the unsigned content certificates. This file is then PGP encrypted and e-mailed to the AACS License Authority. In return the licensing authority will send back a PGP encrypted Singed Content Certificate. Selecting this option will open a standard file save dialog allowing the user to choose the output location.

Signing an Image

1. Right-click on the image to be signed.
2. In the popup menu that appears, select Convert to Type C. This will open a window prompting for an AACS Content Signing Order file. This is the file that is returned from AACS LA.

Note that the file returned from AACS LA is PGP encrypted. If you do not have PGP installed and setup in the CMU on the local computer, then you must first decrypt the file prior to signing an image.

3. After selecting an AACS Content Signing Order File you will be prompted for an MKB file.

   Keep in mind that the MKB Order files purchased from AACS LA contain many individual MKBs. These must be extracted from the file before using.
4. After selecting an MKB file, the CMU will apply the CC files onto the image. This 'signing' process converts the image from a Type B to a Type C.

Troubleshooting

Several log files are now being created to help track problems when signing or extracting a content certificate. Every folder that is being monitored will create a log file with information about the images contained under it. In addition there will be logs in the individual image folders with additional information. Below is a description of what these files record and in which situation they will be useful:

CMU Log Files

Directory/Log File	Description
Directory being monitored	Logs information for any activity on any of the images contained in this folder.
MONITOR.CMU	
Image directory	Logs information specific to the image.
AUTO.CMU	When running in automation, this file contains information regarding auto-signing of the image.
CCOUT.CMU	This file contains information regarding the extraction of the Content Certificate files from the image.
CCIN.CMU	This file logs information during signing of an image (i.e. when the signed CC is applied to the image).
\MKBInBox	Logs conversion results when converted from MKB to FMT. A new log is created every day.
AUTO_YYMMDD.CMU	
\CCInBox	Logs automatic image signing process results. A new log is created every day.
AUTO_YYMMDD.CMU	

If the need to contact Eclipse Support to diagnosis an issue please include as much information as possible. Including the above files in the initial correspondence will speed up our response time.

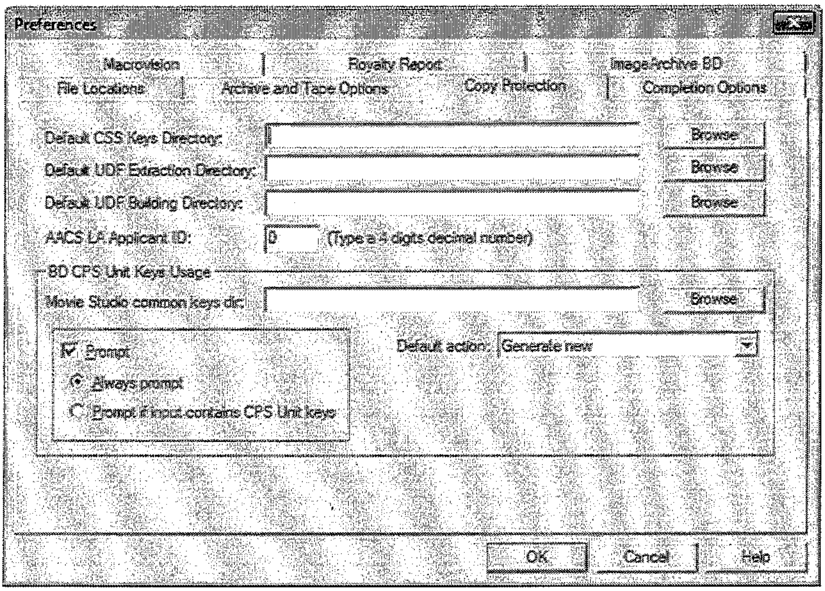
This page has been left blank intentionally.

Re-Using Encryption Keys

When images are encrypted with AACS, each CPS Unit (i.e. group of Titles) is encrypted with a unique encryption key that is generated by ImageCopy during the encryption process. If the same original unencrypted image is sent to different mastering facilities, this will result in different encryption keys being generated during encryption. While this is normal and does not cause any problems, it may present a problem for BD-Live images that include downloadable content.

BD-Live is a feature of Blu-ray Video which gives end-users the ability to download content from an online server. The online-content is part of an existing CPS Unit in the image. Therefore, if the CPS Unit is to be encrypted, then the online content is required to be encrypted using the same encryption key.

There may be other reasons for users to want to use the same encryption keys. This section describes the different methods offered by ImageCopy via its Copy Protection Preferences.


Preferences
Macrovision
Royalty Report
ImageArchive BD
File Locations
Archive and Tape Options
Copy Protection
Completion Options
Browse
Browse
Browse
BD CPS Unit Keys Usage
Browse
OK
Cancel
Help

Default CSS Keys Directory:
Default UDF Extraction Directory:
Default UDF Building Directory:
AACS LA Applicant ID: 0 (Type a 4 digits decimal number)
Movie Studio common keys dir:
☑ Prompt
● Always prompt
○ Prompt if input contains CPS Unit keys
Default action: Generate new

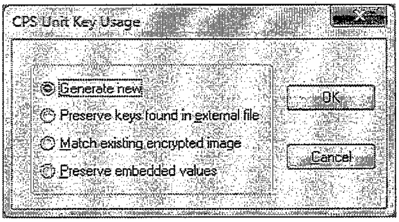
Figure 4: ImageCopy Copy Protection Preferences

Generating the Encryption Keys at Authoring

One method for ensuring that the same encryption keys are used every time an image is mastered is for authoring to generate the encryption keys and supply them with the image to the mastering facility. There are two ways this can be done.

Embedding Title Keys in Image

The encryption keys are stored in the Unit_Key_RO.inf file in the image. Authoring can generate and store the keys in this file. When the image is submitted to a mastering facility, users must tell ImageCopy to use the existing keys. In the ImageCopy Preferences, users should enable the prompt option so that ImageCopy can prompt the user. When the image is processed with ImageCopy, the user will see the following prompt.



CPS Unit Key Usage

● Generate new
○ Preserve keys found in external file
○ Match existing encrypted image
○ Preserve embedded values

In this case, the user needs to choose **"Preserve embedded values"**. This will cause ImageCopy to use the existing encryption keys to encrypt the image.

Using Keys from External File

Rather than embedding the encryption keys in the image, authoring may decide to supply the keys in an external file. The file must be the same Unit_Key_RO.inf file found in the image but with the encryption keys. In this case, the user will choose **"Preserve keys found in external file"**. This will cause ImageCopy to prompt the user for the file if it is not found in the local directory.

Re-Using a Type C Image

There is another method that can be used if the image is not being sent to different replicators at the same time.

A feature of the BDCMF specifications is the ability to send the encrypted and signed Type C image back to the customer in case they want to have it replicated again in the future. Customers can request from mastering facilities a copy of the encrypted and signed Type C image. This allows customers to send the Type C image to any other replicator. Since the image is already encrypted, the encryption keys do not have to be re-generated.

NOTE
The BDCMF specifications allow the creation of a BDCMF Type AX image. This Type of image is the original unencrypted Type A but with Partial Information. The partial information includes the encryption keys that were used to encrypt the image and the signed Content Certificate. Customers can re-submit the Type AX image for mastering in which the same encryption keys are used.

While this option is available, the BDCMF specifications recommend returning of a Type C image back to the customer. Creation of the Type AX image can be done via the CMU.

Using Encryption Keys from Existing Image

Yet another method to ensure the same encryption keys are used is to match the keys of an existing image.

When prompted by ImageCopy (assuming the prompt option is selected in the Preferences), users can select the option to "Match existing encrypted image" and ImageCopy will prompt for the location of the image. Once selected, ImageCopy will extract the encryption keys from the selected image and use them to encrypt the current image.

D Image requirements for re-encrypting using same Signed-CC.

You need to point to a type B, C, or D Image having the original CPSUnitKey. Here is how to modify a SonyCMF image to be usable for this:

Prerequisites:

- • BD CMF "Type A" image that has been converted to Sony CMF and processed by Sony Akane encryption software to a "Type D" image.
- • KVC/VID/KM values available

Process

- • Create a new folder. Take all files, except UD.DAT from BD CMF type A image.

  Add 0000000.DAO file from Sony Type D image.
- • Edit BDCMF.CMF
  - Change <CMFType>A</CMFType> to <CMFType>D</CMFType>
  - Change <File Type="UserData" Name="UD.DAT" ...> to <File Type="UserData" Name="0000000.DAO" ...>
- Edit AACS1.DAT file to include values for KCD, KM, and VID.

  These entries are found in the last section of the aacs1.dat file and confirm to the syntax shown here: (these are not actual values)

```
</ClipAV>
<KCD> ZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ </KCD>
<Km> ZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ </Km>
<Kmv></Kmv>
<VID>ZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ</VID>
</AACSInfo>
```

Result

This image can be used with ImageVerify, ImageEncoder or with ImageCopy to encrypt with the same CPS_Unit key.

- Media Key Block Order Files and valid signed certificates. Both are required for signing images.

  The Media Key Block (MKB) file provides device revocation data as a means to protect content from players which have been compromised.

  The MKB file is obtained from the licensing entity AACS LA LLC. AACS LA will provide licensed manufactures the ability to purchase this mandatory MKB file.

Signed Certificate: this is the file received back from the AACS LA

Unsigned content certificates are extracted from the encrypted image using the CMU. After these files are extracted they are encrypted and sent to AACS LA for signing.

'AACS LA LLC is a licensing company who provides the tools to properly encrypt Blu-ray optical disc with AACS encryption.
http://www.aacsla.com

ImageArchive BD

ImageArchive BD is a new option that can be purchased for EclipseSuite 5.0 BD.

Due to the size of Blu-ray images, users normally have to backup the images to DLT, LTO or hard disk, unlike a CD/DVD image which can be recorded on to a DVD-R disc. Backup and restore to/from a DLT or LTO can be a very slow process. Backing up and restoring to/from hard disk is a lot faster but it is not practical since hard disks can develop bad sector.

ImageArchive BD option allows users to backup to a database specific data from a Blu-ray image. Instead of backing up the image to DLT, LTO or hard disk, users can store a replicated disc instead. When restoring the image, users can use the replica as the source and ImageCopy will use the image data from the database and replica to re-create a Type C image that the user can use to master.

Contact Eclipse Sales or your local distributor for more details on this option.

This page has been left blank intentionally.

Rules & Exclusions

The following are the new rules and exclusions in EclipseSuite BD 5.0. The rest of the manual describes ALL the Blu-ray rules.

Rule Title	Severity	Category	Rule ID
Application location at layer break	Info	Blu-ray	1891
BD Type P Layers resized	Flag	Blu-ray	1899
BD+ SVM file contains all zero data	Error	Blu-ray	1887
BDCMF Type P TL	Info	Exclude	1900
BD-Data	Info	Exclude	1888
BD-Video	Info	Exclude	1889
ImageArchive BD base directory does not match target	Flag	Blu-ray	1893
ImageArchive base directory overridden	Flag	Blu-ray	1894
Missing BDCMF LayerInfo L1SectorSize attribute	Error	Blu-ray	1901
No Playing Time specified	Warning	Blu-ray	1903
Triple layer (Opposite Track Path)	Info	Exclude	1902

3D BD

This is an informational rule that identifies a Blu-ray 3D image.

A 3D Blu-ray image is identifies with one of the following:

1. The **SS_Content_exist_flag** is set in the AppInfoBDMV structure of the Index.bdmv file.
2. At least one SSIF file exists in the \STREAM\SSIF folder.
3. A Clip Information file identifies a video stream that is of type 'MPEG-4 MVC Dependent view'.
4. A 3D-ready PlayList exists.
5. BDCMF version 1.19 or later is detected and the 3D flags are set in the BDCMF.CMF file.

Type:	3D-BD
Reference:	3D BD Specifications
Default Program Action:	Flag

Rule ID: 1721

3D Dependent clip not included in a PlayList

A 3D Dependent clip file is included but not referenced in any PlayList.

Background

The video output on a 3D Blu-ray Video image is composed of base view and dependent view for the left eye and right eye respectively. For each Clip AV Stream file there is a matching Clip Info file that describes it. The Clip Info file specifies whether the matching Clip AV Stream file is part of a 3D video stream. A 3D PlayList contains references to both the base and dependent view clip files.

This condition indicates that a 3D PlayList did not include any references to a Clip AV Stream file. In other words, a 3D Clip AV Stream file has been included but it is not referenced during playback.

Additional Info

When this rule is triggered, the **Additional Info** in the Analysis will display the following message.

Clip information file for '[*ClipAVFile*]' contains ProgramInfo_SS()

The presence of the ProgramInfo_SS structure in a Clip AV Stream file indicates that the file contains video stream data for 3D.

Severity

This condition is considered only a WARNING since it may be possible that it was done intentionally by the author.

Cause

This condition is created by the author or authoring system.

Solution

Consult with the author of the image to see if it is something that was done intentionally.

Type:	3D-BD
Reference:	N/A
Default Program Action:	Warning

Rule ID: 1875

3D ready PlayList file not included

The image is identified as a 3D BD image but a 3D-ready PlayList has not been included.

Background

In a Blu-ray Video, a PlayList file includes PlayItems, which contain references to Clip AV Stream files (*.M2TS). A 3D-ready PlayList is one that includes PlayItems which contain references to Stereoscopic Interleaved files (*.SSIF). This rule is triggered when an image is identified as a 3D BD but no 3D-ready PlayLists are found. This condition may also occur if SSIF files exist but no 3D-ready PlayList that references them.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display more details with one of the following messages.

But Index Table file 3D content flag set

*The **SS_content_exist_flag** in the Index Table File (index.bdmv) identifies the image as a 3D BD but the image does not include a 3D-ready PlayList file.*

But SSIF file(s) detected

The image include Stereoscopic Interleaved files (\STREAM\SSIF\*.SSIF), indicating that the image may be a 3D BD. However, the image does not include any 3D-ready PlayLists, which would reference these files.

Severity

This condition is considered an ERROR since it is not clear if the image was intended to be a normal Blu-ray Video (2D) or a 3D Blu-ray Video.

Cause

This problem is normally caused by the authoring system that created the image.

Solution

The image must be re-authored to correct this problem.

Type:	3D-BD
Reference:	3D BD Specifications
Default Program Action:	Error

Rule ID: 1725

AACS

This rule is triggered when the Eclipse software identifies the Advanced Access Content System (AACS) copy protection that is used in the Blu-ray video format.

Type:	Exclude
Reference:	N/A
Default Program Action:	Info

Rule ID: 833

AACS LA pre-recorded MKB

This is an informational message that identifies the presence of a pre-recorded MKB file on a BD image.

Type:	Exclude
Reference:	N/A
Default Program Action:	Info

Rule ID: 1845

AACS LA recordable MKB

This is an informational message that identifies the presence of a recordable MKB file on a BD image.

Type:	Exclude
Reference:	N/A
Default Program Action:	Info

Rule ID: 1846

AACS LA signature verification error

The AACS LA signature is invalid.

Background

The AACS specifications require that analysis tools such as EclipseSuite and CMU validate the AACS signature on files that are signed by AACS LA. These files include the Content Certificate (CC), Content Hash Table (CHT) and Media Key Block (MKB). The same requirement applies to Blu-ray players when playing back a Blu-ray Video from disc.

The signature validates the authenticity of these files. If the signature validation fails on any of them, it could indicate file corruption or that the file may have been hacked.

When a BDCMF image is signed, the CC and MKB files are replaced with "signed" files that are received from AACS LA. These files include a signature that can be verified to ensure that no corruption has occurred during the transmission of the files from AACS LA or during the image signing process.

Additional Info

When this rule is triggered, the **Additional Info** column in the analysis will identify the file whose signature has failed.

\AACS\Content000.cer

This condition indicates that the AACS LA signature in the content certificate file for layer 0 is invalid.

\AACS\Content001.cer

This condition indicates that the AACS LA signature in the content certificate file for layer 1 is invalid.

\AACS\ContentRevocation.lst

This condition indicates that the AACS LA signature for the content revocation list file is invalid.

Severity

This rule is considered an ERROR since it indicates file corruption, which may affect playability.

Cause

This type of problem is typically caused by corruption of the file. The files are normally PGP-encrypted and sent via an email from AACS LA. File corruption can occur when un-encrypting and copying the files to the system that is used to sign the image.

Solution

Since the problem typically occurs due to file corruption, making a new copy of the files usually fixes the problem. For example, if you still have the email from AACS LA that contains these files, download a new copy of the files from the email and use that instead. If the same problem occurs, then it may indicate that the corruption occurred elsewhere.

Note that this problem may also indicate physical defects on the hard disk or the medium used to copy the files.

Type:	Blu-ray
Reference:	AACS Specifications
Default Program Action:	Error

Rule ID: 1526

AACS Managed Copy Manifest File error

An error occurred while processing the Managed Copy Manifest File.

Background

The AACS specifications require that images that are Managed Copy ready include the Managed Copy Manifest File (mcmf.xml). During the analysis, the EclipseSuite programs check to make sure the file is present. If it is found, then it is loaded into memory and its contents are analyzed. This rule indicates that the EclipseSuite tools were unable to load the file for analysis or an error parsing the contents of it.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display more details with one of the following messages.

Failed to alloc memory for '[*Filename*]'

This condition indicates a system problem. The EclipseSuite programs were unable to allocate memory when loading the Managed Copy Manifest file. The file will not be analyzed. This might occur if there are not enough resources (memory) available in your computer to load this file. Try closing some applications before running the job again.

mcmf.xml File Format: [*Error_Description*]

This condition indicates that an error occurred while parsing the Managed Copy Manifest file. The Error_Description may provide more details as to the line and column number within the file where the error occurred.

The AACS specifications define the schema of the Managed Copy Manifest file. This condition indicates that the Managed Copy Manifest file on the image does not conform to the schema defined in the specifications.

Severity

The Managed Copy Manifest file is required for images that are Managed Copy ready. This rule indicates possible file corruption or a system error. Since it does not necessarily indicate a problem with the image, this condition is treated as a WARNING.

Cause

If the **Additional Info** message indicates a memory allocation problem then it may be a program or system error. Otherwise, the problem is related to parsing the content of the file. In that case, it might indicate that the file was not formatted correctly during authoring.

Solution

If the message in the **Additional Info** column is a parsing error, then contact the authors of the image as this would indicate that the file is not formatted correctly. Otherwise, contact Eclipse Customer Support for further assistance.

Type:	Blu-ray
Reference:	AACS Specifications for Blu-ray
Default Program Action:	Warning

Rule ID: 1720

AACS XML Formatting Error

A required XML element or attribute is missing from the AACS1.DAT file.

Background

The AACS1.DAT file is included with BDCMF images using BDCMF Version 0.90 and earlier. On a Type A image, this file contains a list of the Clip AV files. Each File entry identifies a file, start address, size and the CPS Unit that is assigned to the file. Each File entry also includes a list of Extents that make up the file. The CPS Unit number identifies the encryption key used to encrypt the sectors specified by the Extents of each file. All of this information is recorded in the element called `<CLIPAV>`.

The information in this file is critical for the encryption of the image. Therefore, this rule only applies to images that are Type A. After the image is encrypted (Type B or later), the <CLIPAV> element may be removed from the file. However, if it is left in the file, it should be ignored by applications.

Below is a sample AACS1.DAT file for a Type A image:

```
<?xml version="1.0" encoding="UTF-8"?>
<AACSInfo xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="BDCMFschema.xsd">
    <ClipAV>
        <NumOfCPSUnit>1</NumOfCPSUnit>
        <File Type="ClipAVStream" Name="00000.m2ts" Access="Extent" >
            <CPSUnitNo>1</CPSUnitNo>
            <Extent Start="2865" Size="524256" />
            <Extent Start="526941" Size="524256" />
            <Extent Start="1051197" Size="524256" />
            <Extent Start="1575453" Size="524256" />
            <Extent Start="2099709" Size="524256" />
            <Extent Start="2623965" Size="524256" />
            <Extent Start="3148221" Size="524256" />
            <Extent Start="3672477" Size="524256" />
            <Extent Start="4196733" Size="524256" />
            <Extent Start="4720989" Size="524256" />
            <Extent Start="4720989" Size="524256" />
            <Extent Start="5245245" Size="524256" />
            <Extent Start="5769501" Size="524256" />
            <Extent Start="6293757" Size="524256" />
            <Extent Start="6818103" Size="524256" />
            <Extent Start="7342269" Size="524256" />
            <Extent Start="7866525" Size="524256" />
            <Extent Start="8390781" Size="524256" />
            <Extent Start="8915037" Size="524256" />
            <Extent Start="9963549" Size="326310" />
        </File>
        <File Type="ClipAVStream" Name="00001.m2ts" Access="Extent" >
            <CPSUnitNo>1</CPSUnitNo>
            <Extent Start="109289859" Size="151878" />
        </File>
        <File Type="ClipAVStream" Name="00002.m2ts" Access="Extent" >
            <CPSUnitNo>1</CPSUnitNo>
            <Extent Start="10441737" Size="524256" />
            <Extent Start="10965993" Size="58080" />
        </File>
    </ClipAV>
</AACSInfo>
```

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display the XML element or attribute in question with one or more of the following messages.

No ClipAV element defined

This message is displayed when the required element <CLIPAV> is not present in the AACS1.DAT file. The information in this file is used by AACS encryption tools, such as ImageCopy, when applying AACS encryption to an image. Without the Clip AV element, it may be impossible to process the image. The <ClipAV> element is required only for Type A images. Once the image has been encrypted (Type B or later), this condition should not occur or can be ignored.

Number of CPS Units missing

This message is displayed when the required element <NUMOFCPSUNIT> is missing. This element specifies the number of CPS Units in the BD image. Each Clip AV file is assigned to a CPS Unit. The CPS Unit number assigned must be a value ranging from 1 to the value specified by <NUMOFCPSUNIT>. A CPS Unit determines the encryption key that will be used to encrypt a Clip AV file. Therefore, the CPS Unit value assigned to a Clip AV file cannot be larger than the Number of CPS

Units.

No ClipAVStream attribute defined in File Tag

This message is displayed when a `<File>` *element is missing the attribute* `Type="ClipAVStream"`*. This attribute identifies the file as a Clip AV Stream file (*.m2ts), which is the only type that should be specified in the AACS1.DAT file.*

CPSUnitNo child element missing from File Tag

This message is displayed when a <File> element is missing the child element `<CPSUnitNo>`*. Every File element must have a* `<CPSUnitNo>` *child element. The* `<CPSUnitNo>` *element specifies the CPS Unit number that is assigned to the File. The CPS Unit number specifies the encryption key that will be used to encrypt the file content.*

No Name element defined in File Tag

This message is displayed when a <File> element is missing the Name="#####.m2ts" attribute. The Name attribute is used to specify the name of the Clip AV stream file (e.g. "00001.mt2s") that is described by the <File> element.

Severity

This rule is considered an ERROR since any missing or invalid element or attribute may cause the image to fail during the encryption process.

Cause

This problem is typically caused by the authoring system that created the image.

Solution

It is likely that the image may have to be re-authored. Contact Eclipse Customer Support for further assistance.

> **NOTE**
>
> *If you are using ImageCopy to process (i.e. to apply AACS encryption) an image with this error then this rule can be ignored. ImageCopy does not rely on the information from the AACS1.DAT file. The UDF file system in the image contains the same information as this file. ImageCopy will parse the UDF file system and use that instead. However, this is not true of other encryption tools. If the image is to be encrypted using other tools, then this condition should be considered serious as it will likely cause the encryption to fail.*

Type:	DDP
Reference:	BD CMF Version 0.90 Section 4
Default Program Action:	Error

Rule ID: 845

All zero bytes dstring value

A dstring field contains all zeros.

Background

dstring fields defined by the ECMA-167 specifications contain a string value and a length. The ECMA-167 specifications state that, unless otherwise specified, a dstring should not contain all zeros. In other words, the dstring should hold some data other than 0's.

ECMA-167 provides a base file system specification from which others, like UDF, derive. The UDF file system specifications re-define the dstring fields and allow them to be set to all zero bytes. Therefore, this rule will only apply to media that is based purely on ECMA-167. In CD, DVD and Blu-ray, there are no logical formats which are based purely on ECMA-167. Therefore, in the current EclipseSuite implementation, it is unlikely that this rule will ever be triggered.

> **NOTE**
> This rule is part of the Blu-ray Video Verifier analysis checks. This rule is specific to dstrings as defined in the ECMA-167 specifications. Since no Blu-ray image is based purely on ECMA-167, this rule should never be triggered in the current EclipseSuite implementation. However, future versions of EclipseSuite may perform an ECMA-167 analysis and only then will this rule be triggered.

Severity

This rule defaults to an ERROR severity as recommended by the Blu-ray file system verifier specifications. However, as of the current EclipseSuite implementation, this rule will not be triggered on any Blu-ray Video image since the UDF file system will allow a dstring with zero bytes.

Cause

This condition is caused by the authoring system that created the image.

Solution

Currently this rule should never be triggered. If it does, contact Eclipse Customer Support for further assistance.

Type:	UDF
Reference:	ECMA 167 1/7.2.12, BD-ROM U00-004
Default Program Action:	Error

Rule ID: 1804

An AACS related file could not be loaded or read

The EclipseSuite tools were unable to find or load the Content Certificate (CC) or Content Hash Table (CHT) files.

Background

All Blu-ray images include a Content Certificate and Content Hash Table file for each layer in the image. The CHT contains hashes for each of the Clip AV files. The hashes in the CHT are hashed again and the hash values are stored in the Content Certificate file. Hash values are used to validate the integrity of files in a Blu-ray image. During playback, a Blu-ray player is required to validate a number of the hash values. Similarly, during analysis of a Blu-ray image, the EclipseSuite tools recalculate all hashes and compare them to the hashes in the CHT and CC. When this error occurs, it indicates that the EclipseSuite tools were not able to find the CC or CHT files or a problem occurred when attempting to load the file into memory. Additional errors may appear because of this error.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display the file that it couldn't find or failed to load.

\AACS\Content000.cer

This message appears when analyzing a dual-layer BD image and the EclipseSuite tools are attempting to find and load the content certificate file for layer 0 (Content000.cer). When this occurs, additional errors and/or warnings may appear. It is also possible that the job may not be able to continue and abort.

\AACS\Content001.cer

This message appears when analyzing a dual-layer BD image and the EclipseSuite tools are attempting to find and load the content certificate file for layer 1 (Content001.cer). When this occurs, additional errors and/or warnings may appear. It is also possible that the job may not be able to continue and abort.

\AACS\ContentHash000.tbl

This message appears when the EclipseSuite tools are unable to find or load the contents of the Content Hash Table file for layer 0. When this occurs, additional errors and/or warnings may appear. It is also possible that the job may not be able to continue and abort.

\AACS\ContentHash001.tbl

This message appears when the EclipseSuite tools are unable to find or load the contents of the Content Hash Table file for layer 1. When this occurs, additional errors and/or warnings may appear. It is also possible that the job may not be able to continue and abort.

NOTE

The EclipseSuite debug information may be able to indicate whether this rule was triggered due to a failure when loading the file into memory or due to an error finding the file. Depending on the message displayed in the Additional Info column, you can activate the Debug window in the EclipseSuite applications and search for one of following messages:

Error finding Layer 0 content hash table
Error finding Layer 0 content certificate file!
CBDPlayer: Error finding Layer 0 CC file!
Error finding Content certificate file on Layer 1
Failed to load Content Certificate layer 1
CBDPlayer: Error finding Layer 1 CC file!

Severity

This condition is considered an ERROR since it may lead to playability problems.

Cause

It is unknown as to the cause of this condition.

Solution

Please contact Eclipse Customer Support. It is likely that a log file showing these errors will be required in the troubleshooting of this condition. Please email the log file to Eclipse Support with your questions.

Type: Blu-ray
Reference: N/A
Default Program Action: Error

Rule ID: 1546

Anchor Volume Descriptor Pointer

This is an informational rule that identifies the location of an Anchor Point.

Additional Info

When this rule is triggered, the **Additional Info** column in the analysis will display the location where the Anchor Points were found.

Found at LSN [x]

This message identifies the location where an Anchor Point was found. Normally, there should be two anchor points recorded: one at logical sector 256 and the other at the last logical sector on the media. Only the one at logical sector 256 is required.

Type: UDF
Reference: ECMA 167 & UDF
Default Program Action: Note

Rule ID: 1427

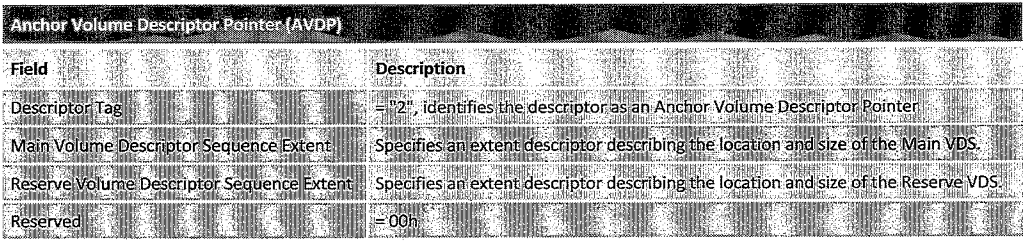
Anchor Volume Descriptor Pointer at unexpected location

An Anchor Point was found at an incorrect location.

Background

An Anchor Point contains information that may be used to identify the volume on a disc. It also provides the location and length of the Main and Reserve Volume Descriptor Sequences, which are the entry point into the file system on a disc. Without the Main Volume Descriptor Sequence, it is not possible to read the contents of a disc. Therefore, finding the Anchor Point is critical in the readability of a disc's content.

An Anchor Volume Descriptor Pointer is identified by an Anchor Point. An Anchor Point is recorded at logical sector 256 and optionally the last sector of the media. When this rule is triggered, it indicates that an Anchor Point (and Anchor Volume Descriptor Pointer) was found at a sector location that is not 256 or the last sector of the media.



Anchor Volume Descriptor Pointer (AVDP)

Field	Description
Descriptor Tag	= "2", identifies the descriptor as an Anchor Volume Descriptor Pointer
Main Volume Descriptor Sequence Extent	Specifies an extent descriptor describing the location and size of the Main VDS.
Reserve Volume Descriptor Sequence Extent	Specifies an extent descriptor describing the location and size of the Reserve VDS.
Reserved	= 00h

Severity

This condition is typically not a serious problem as long as the primary Anchor Point at logical sector 256 is found. Any additional copies of the Anchor Point are redundant and only used if the first one is defective.

Possible Cause

This problem is caused by the authoring system or application that created the image.

Possible Solution

This type of problem may be corrected by re-authoring the image. However, this is not necessary as long as the primary Anchor Point at logical sector 256 is found.

Type:	UDF
Reference:	ECMA 167
Default Program Action:	Warning

Rule ID: 1515

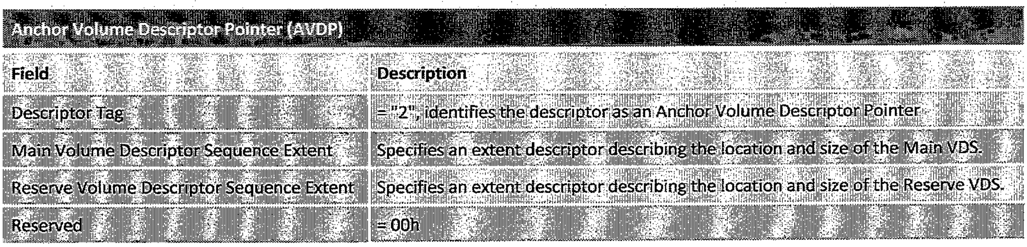
Anchor Volume Descriptor Pointer expected at Logical Sector

An Anchor Volume Descriptor Pointer (AVDP) was not found at the expected location.

Background

An AVDP contains information that may be used to identify the volume on a disc. It also provides the location and length of the Main and Reserve Volume Descriptor Sequences, which are the entry point into the file system on a disc. Without the Main Volume Descriptor Sequence, it is not possible to read the contents of a disc. Therefore, finding the Anchor Point is critical in the readability of a disc.

An Anchor Volume Descriptor Pointer is identified by an Anchor Point. An Anchor Point is recorded at logical sector 256 and optionally the last sector of the media. When this rule is triggered, it indicates that an Anchor Point (and Anchor Volume Descriptor Pointer) was found at a sector location that is not 256 or the last sector of the media.



Anchor Volume Descriptor Pointer (AVDP)

Field	Description
Descriptor Tag	= "2", identifies the descriptor as an Anchor Volume Descriptor Pointer
Main Volume Descriptor Sequence Extent	Specifies an extent descriptor describing the location and size of the Main VDS.
Reserve Volume Descriptor Sequence Extent	Specifies an extent descriptor describing the location and size of the Reserve VDS.
Reserved	= 00h

Additional Info

When this rule gets triggered, the **Additional Info** column in the Analysis will display more details with one of the following messages.

ECMA167: at [*location*] for Medium Interchange Level 1

The Anchor was expected at logical sector 256 or N-256, where N is the last sector of user data. The Anchor Point at 256 is *the primary Anchor Point which all players will look for. If this is not recorded then players will normally look at any of the backup locations (last logical sector and last logical sector - 256).*

If this message refers to the Anchor Point at logical sector 256 then this condition can be considered an ERROR.

DVD-ROM: at [*location*]

On a DVD-ROM, the Anchor is expected at logical sector 256. This condition can be considered an ERROR *since the Anchor Point at logical sector 256 is the primary Anchor Point.*

DVD-ROM: at [*location1*] or [*location2*]

On a DVD-ROM, the Anchor was expected at logical sector N or N-256, where N is the last user data sector. This condition is not considered serious since it refers to backup copies of the Anchor Point.

at [*location*]

On a BD-ROM, the Anchor is expected at logical sector 256, N-256 and N, where N is the last user data sector. If this message refers to the Anchor Point at location 256, then it can be considered an ERROR. *If it refers to an Anchor Point at any other location, then it is not considered serious.*

Severity

This condition is typically not a serious problem as long as the primary Anchor Point at logical sector 256 is found. Any additional copies of the Anchor Point are redundant and only used if the first one is defective.

Possible Cause

This problem is caused by the authoring system or application that created the image.

Possible Solution

This type of problem may be corrected by re-authoring the image. However, this is not necessary as long as the primary Anchor Point at logical sector 256 is found.

Type:	UDF
Reference:	Blu-ray and DVD-ROM File System Specifications
Default Program Action:	Warning

Rule ID: 706

Anchor Volume Descriptor Pointer in rewritable or overwritable partition

The EclipseSuite tools have determined that the Anchor Volume Descriptor Pointer is recorded in a volume space which has been allocated for a Rewritable or Overwritable partition.

Background

An Anchor Volume Descriptor Pointer is a structure that contains pointers to locations of the Main and Reserve Volume Descriptor Sequences. According to the ECMA 167 Specifications, it should not be recorded in a Rewritable or Overwritable partition.

A Main Volume Descriptor Sequence contains one Primary Volume Descriptor which identifies the file system and its properties. Playback systems use the Anchor Volume Descriptor Pointer to find out the location of the Primary Volume Descriptor. If it is recorded in a Rewritable or Overwritable partition, it could be erased and the disc may become unplayable.

Note also that Read-Only media (i.e. a replicated disc and DDP/CMF images) should not contain any Rewritable or Overwritable partitions. These may only be present on recordable/rewritable media.

Type:	UDF
Reference:	ECMA 167 3/28.5
Default Program Action:	Error

Rule ID: 695

Application location at layer break

This is an informational message that identifies the playtime address at the layer break. The playtime will be displayed in the Additional Info column.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Info

Rule ID: 1891

Application Root Certificate

This is an informational message that identifies a BD-J Application Root Certificate. The certificates are used to authenticate BD-J Applications. When this rule is triggered, the certificate number will be displayed in the **Additional Info** column of the Analysis.

Type:	Blu-ray
Reference:	Blu-ray Disc Read-Only Format Part 3: Audio Visual Basic Specifications
Default Program Action:	Info

Rule ID: 1619

ATC duration of EXT1 is less than 300 milli-seconds

The duration of a 3D extent is less than 300 milliseconds.

Background

The Blu-ray Video specifications for 3D define several rules that must be followed. One of these requires that all extents of the base 3D file be equal or greater than 300 milliseconds except on the last extent.

Severity

It is unknown how this may affect playability. Nevertheless, it is considered an ERROR since it is a requirement of the specifications.

Cause

This problem is caused by the authoring system that created the image.

Solution

The image must be re-authored. Contact Eclipse Support for further assistance.

Type:	3D-BD
Reference:	Blu-ray Disc Read-Only Format Part 3: Audio Visual Basic Specifications (3-1 Core Specifications) Annex P Main requirements for Stereoscopic 3D
Default Program Action:	Error

Rule ID: 1785

Authentication message attribute case mismatch

An attribute in the Signature File does not use the correct character casing.

Background

According to the JAR File Specifications, the version attributes of the Signature File are case sensitive.

The JAR Specifications define the optional 'Magic' attribute. The use of this attribute is defined by the applications (such as BD-Java) that implement the JAR Specifications. Although the current Blu-ray specifications do not support the use of 'Magic' attributes, BD-Java requires that the Signature-Version attribute be in the correct format since future version may use the Signature-Version as a 'Magic' string.

Additional Info

When this error occurs, the **Additional Info** column in the Analysis will display more details with the following messages.

'[*JARFile*]', '[*SignatureFile*]', expecting 'Signature-Version' instead of '[*ActualVersionAttr*]'

This condition indicates that the ***Signature-Version*** *attribute was specified but it is not capitalized as specified above. It is case sensitive so it must be specified as:*

`Signature-Version`

'[*JARFile*]', '[*SignatureFile*]', expecting 'BDJ-Signature-Version' instead of '[*ActualBDJVerAttribute*]'

This condition indicates that the ***BDJ-Signature-Version*** *attribute was specified but it is not capitalized as specified above. It is case sensitive so it must be specified as:*

`BDJ-Signature-Version`

'[*JARFile*]', '[*SignatureFile*]', expecting 'SHA1-Digest-Manifest' instead of '[*ActualSHA1DigestAttribute*]'

This condition indicates that the ***SHA1-Digest-Manifest*** *attribute was specified but it is not capitalized as specified above. It is case sensitive so it must be specified as:*

`SHA1-Digest-Manifest`

Severity

The BD-Java specifications indicate that the Signature-Version attribute may be used as a 'Magic' string. However, this is not supported in the current Blu-ray specifications. Therefore, this condition is only a WARNING.

Cause

This problem is caused by the authoring application that created the image.

Solution

This condition indicates a problem with the authoring application. Contact the manufacturer of the authoring application for assistance.

Type:	Blu-ray
Reference:	Blu-ray Disc Read-Only Format Part 3: Audio Visual Basic Specifications (3-2 BD-J Specifications) Section 12.3.1: Authentication of Signed JAR File
Default Program Action:	Warning

Rule ID: 1643

AV Stream File not recorded as Real-Time

Real-Time files are files that require a minimum data transfer rate when reading or writing (e.g. audio and video data). Real-Time files are identified by a File Type of 249 in the File Type field of the file's ICB. In BD-ROM, any file recorded in a Stream Directory (i.e. in the \STREAM folder) is expected to be a Real-Time file. When this rule is triggered, it indicates that the EclipseSuite tools found a file in the \STREAM directory that is not identified as a Real-Time file.

Additional Info

When this rule is triggered, the **Additional Info** column in the analysis will identify the file in question.

AV Stream File [*filename*]

This message identifies the file that was found in the Stream Directory but is not identified as a real-time file (i.e. File Type is not 249).

Type:	UDF
Reference:	BD-ROM U05-018, UDF 2.50 6.11
Default Program Action:	Error

Rule ID: 806

Bad Title Structure Component

The Title Structure file is not formatted properly.

Background

A Title Structure file is a file that defines the authoring layout of a Blu-ray image. Eclipse has created the title structure file so that a movie studio can create a custom layout that meets their authoring requirements for Blu-ray. Once this title structure is defined, the Eclipse software checks the image to make sure it complies with the title structure requirements.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display more details about the condition that triggered this rule.

Severity

This error indicates that the image being analyzed did not conform to the title structure requirements. Therefore, this condition is considered an ERROR. However, the Title Structure file gives organizations the ability to define the severity of most conditions that triggers this rule. Therefore, the default severity of this rule may be overridden by the Title Structure file being used.

Cause

This condition is normally caused during authoring of the image.

Solution

This error does not indicate any problem with the Blu-ray format. It is an error that gets triggered when the layout of the image does not conform to a predefined layout specified by the movie studio. Check with the author or movie studio whether it is ok to continue with the image or whether it should be re-authored.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

Rule ID: 1608

BCA

This is an informational message identifies whether the BCA flag on an image or disc is set.

Background

The BCA is used for the recording of information such as serial numbers and Barcode information that can uniquely identify an image. It can also be made so that each replica of a title can be unique. BCA is optional for both DVDs and Blu-ray.

> **NOTE**
>
> *Currently, on a DVD, the EclipseSuite tools trigger this rule only on DVD replicas that contain valid BCA information. It will not be triggered on DVD images on DLT or hard disk.*

Type:	Exclude
Reference:	DVD Part 1 - Physical Specifications pg. PHX-16 BD-ROM Part 1: Chapter 9 Layer0, 21.30 – 22.0mm (optional)
Default Program Action:	Info

Rule ID: 260

BCA Override

This is an informational message indicating that the BCA flag in the PIC.DAT file has been overridden.

Background

BCA is a flag in the PIC data during the lead-in. On a replicated disc, it indicates whether a BCA is recorded on the disc. On a BDCMF image, it indicates whether the BCA needs to be recorded by the encoder or off-line BCA writer.

When using an Eclipse encoder, users can override the BCA flag on the PIC data to either ON or OFF. This is done via the **OverridePICBCAFlag** parameter in the BI file.

```
[General]
...
OverridePICBCAFlag = [ON]|[OFF]
...
```

Additional Info

The **Additional Info** column in the Analysis will indicate whether it is being forced ON or OFF.

Type:	Exclusion
Reference:	N/A
Default Program Action:	Flag

Rule ID: 1663

BD Archive error

An error occurred during a restore operation of a Blu-ray image.

Background

When restoring a BDCMF image, ImageCopy uses a replica and matching ImageArchive database record to generate a Type C BDMCF image. During this process, there are several conditions that can trigger this error. Refer to the Additional Info column in the analysis and contact Eclipse Customer Support for assistance.

Additional Info

When this rule is triggered, the **Additional Info** column in the analysis will display one of the following messages.

Failed to set BDCMF 'NumOfCPSUnit' value
File '\\AACS\\MKB_RO.inf' not found
Failed to load '\\AACS\\MKB_RO.inf'
Reference record version error
Failed to allocate memory for archive operation
Failed to set connection strings. Error [ErrorNo]
Failed to set table names. Error [ErrorNo]

Failed to connect. Error [ErrorNo]
Can't generate first reference record
Can't determine latest reference record
Latest reference record version error
Can't generate latest reference record
Can't get latest reference record
Disc image not in archive
Error [ErrorNo] searching for disc image record
Failed to disconnect. Error [ErrorNo]
No archive data available
Failed to update BDCMF Km
Failed to update BDCMF KCD
Failed to update BDCMF PMKB
No UKRO data available
Critical error handling UKRO data

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

Rule ID: 1847

BD BCA Error

This rule is triggered by the condition where the BCA Descriptor Flag is on, but the BCA information cannot be read from a BD replica.

Background

The BCA Descriptor Flag is set during authoring and is described in the PIC.DAT file of a BDCMF image. The contents of this file are recorded in the PIC Zone of BD discs. The BCA can be written on the glass master, thus resulting in every replica of the same glass master having the same BCA information. Alternatively, the BCA information can be serialized on the replicas after replication, thus resulting in each replica of the same title having a unique ID.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display one of the following messages providing more details.

BCA Flag set, but data could not be read from disc

This message indicates that the BCA Flag is set in the PIC information of the disc. However, a failure occurred when the drive tried to read it.

Severity

This rule is considered an error since this condition has been seen to result in a non-playable disc in PS3 drives. Some replicas have shown the PS3 error code 80029907.

Solution

If the replica is intended to contain BCA, it must be added by re-mastering or applying BCA to the replica.

If BCA is not intended, the image should be re-authored with the BCA flag off or the source PIC data should be modified to change the BCA Descriptor Flag.

Type:	Blu-ray
Reference:	BDCMF Version.90 spec, Appendix D
Default Program Action:	Error

Rule ID: 1458

BD CMF level 0.XX

This rule identifies a Blu-ray image using BDCMF version 0.XX.

Type:	Exclusion
Reference:	BDCMF Specifications
Default Program Action:	Info

Rule ID: 681

BD Hybrid

This rule identifies a Blu-ray Hybrid disc.

Background

A Blu-ray Hybrid is a BD25 disc combined with a legacy DVD5 or CD (including recordable). This can be done since the information for the different formats are on different locations (layers) on the disc.

This rule is triggered on a source BDCMF image. The XML element **\DiscInfo\DiscType** is set to 'CD RO' or 'DVD RO'. The **Additional Info** column will identify which type of layer (CD or DVD) is included with the BD layer.

Type:	Blu-ray
Reference:	BDCMF Specifications, Blu-ray ROM Physical Specifications
Default Program Action:	Flag

Rule ID: 1480

BD PMSN

This rule is used to display the Pre-recorded Media Serial Number (PMSN) value of a BD disc. The PMSN will be displayed in the **Additional Info** column.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Info

Rule ID: 1494

BD Type P Layers resized

This is an informational message that indicates that the layers in a dual-layer Type P Blu-ray image have been resized.

Background

In the replication process, it may sometimes be difficult obtain in-spec signals on the outer diameter of a BD50 disc if layers are filled to the maximum allowed capacity. Since the data on a Blu-ray ROM image (i.e. Type P) does not have any dependencies on the layer number, ImageCopy allows users to move some of the data from layer 0 into layer 1 to balance the data between both layers. This would allow layer 0 to end earlier. This, of course, requires that there is sufficient space available on layer 1.

To allow resizing of the layers of a Type P image, users can enable the behavior "Re-size layers for Type P BDCMF".

Be aware that since both layers will be modified, comparing back to the original image will not be possible.

Type:	Blu-ray
Reference:	None
Default Program Action:	Flag

Rule ID: 1899

BD+

This is an informational message, which is used to identify Blu-Ray images that use the enhanced Content protection system BD+.

Type:	Blu-ray
Reference:	System Description Blu-ray Disc Read-Only Format, Security Virtual Machine, Specifications (BD+). Version 1.00, 31 March 2006
Default Program Action:	Info

Rule ID: 1461

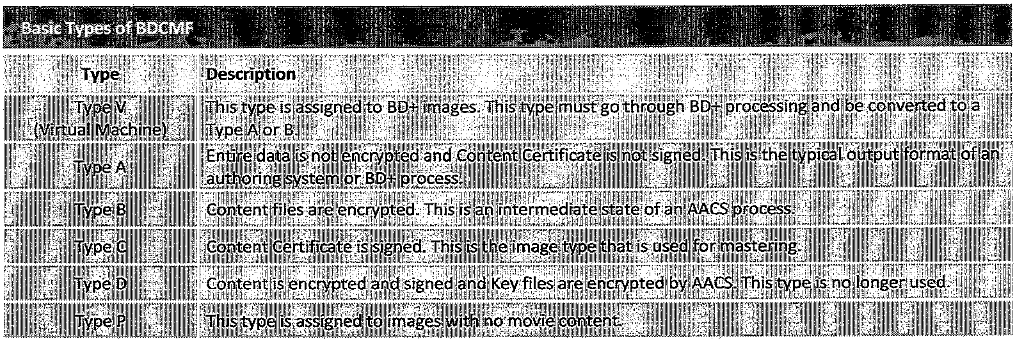
BD+ process required

The Blu-ray image is a Type V, which requires BD+ processing prior to AACS encryption and mastering.

Background

The BDCMF specifications define several different types of BDCMF images. Each specify that image status from authoring to replication. A Type V image requires BD+ processing before it can be introduced in a pre-mastering or mastering environment.

Below is a table that describes the different types.



Basic Types of BDCMF

Type	Description
Type V (Virtual Machine)	This type is assigned to BD+ images. This type must go through BD+ processing and be converted to a Type A or B.
Type A	Entire data is not encrypted and Content Certificate is not signed. This is the typical output format of an authoring system or BD+ process.
Type B	Content files are encrypted. This is an intermediate state of an AACS process.
Type C	Content Certificate is signed. This is the image type that is used for mastering.
Type D	Content is encrypted and signed and Key files are encrypted by AACS. This type is no longer used.
Type P	This type is assigned to images with no movie content.

Severity

This rule is considered an ERROR since the image cannot be processed in premastering or mastering. It doe not indicate a problem with the image. However, this image Type cannot be processed until BD+ is applied. During BD+ processing, the image will be converted to a Type A, which is the typical image Type delivered to a replicator.

Cause

This rule does not indicate a problem with the image. However, it indicates that it has not gone through the BD+ process, which is required for this type of image.

Solution

This image must be returned to the content owner (customer/authoring) so that it can be taken through the BD+ process.

Type:	Blu-ray
Reference:	BDCMF 0.90 Specifications
Default Program Action:	Abort

Rule ID: 1519

BD+ SVM file contains all zero data

The SVM file is part of the BD+ copy protection in Blu-ray Video images and should contain valid data. This error can occur in authoring. However, it can also occur if a user replaces this file via the UDF tab in the EclipseSuite tools.

Type:	Blu-ray
Reference:	None
Default Program Action:	Error

Rule ID: 1887

BD-9

This is an informational message that identifies a BD-ROM image as a BD9. BD-9 refers to Blu-ray data recorded on a DVD substrate.

Type:	Blu-ray
Reference:	BDCMF Specifications
Default Program Action:	Info

Rule ID: 1498

BD-Data

This is an informational message that identifies a Blu-ray ROM image containing only computer data. This is identified via the CONTENTCATEGORY attribute in the BDCMF.CMF file of a BD image.

Type:	Blu-ray
Reference:	None
Default Program Action:	Error

Rule ID: 1888

BD-Video

This is an informational message that identifies a Blu-ray Video image. This is identified via the CONTENTCATEGORY attribute in the BDCMF.CMF file of a BD image.

Type:	Exclude
Reference:	BDCMF Specifications
Default Program Action:	Info

Rule ID: 1889

BDCMF and image content disagree

An unexpected BDCMF image Type was encountered.

Background

BDCMF images have different `CMFType` names to specify the process status of an image (`Type V`, `A`, `B`, `C`, `D` and `P`). The `CMFType` must agree with the `ContentCategory` which describes the type of content included with the image (`'BD-ROM Movie Media'`, `'BD-ROM Media with BD Data'` or `'BD-ROM Data Media'`). This rule is triggered when the `CMFType`, `ContentCategory` and actual image content don't agree.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display more details with one of the following messages.

BDCMF Type is '[*CMFType*]' instead of 'P'

The file system of the image does not conform to the Blu-ray Video file system specifications. Therefore, it is assumed to be a BDCMF image containing computer data only (`ContentCategory="BD-ROM Data Media"`). However, the BDCMF `Type` does not specify a `Type P`. When a BDCMF image does not have movie content, its BDCMF `Type` and `ContentCategory` should be set to '`P`' and '`BD-ROM Data Media`', respectively.

BDCMF 'ContentCategory' is '[*ContentCategory*]' instead of 'BD-ROM Data Media'

The file system of the image does not conform to the Blu-ray Video file system specifications. Therefore, it is assumed to be a BDCMF image containing computer data only (`ContentCategory="BD-ROM Data Media"`). However, the `ContentCategory` does not specify a '`BD-ROM Data Media`'. When a BDCMF image does not have movie content, its BDCMF `Type` and `ContentCategory` should be set to '`P`' and '`BD-ROM Data Media`', respectively.

Unexpected BDCMF Type '[*CMFType*]'

This message indicates that an image with a `Type P`, `Type V` or an unknown type was found. This indicates that the image includes movie content so the EclipseSuite tools were expecting a `Type A`, `B` or `C`.

Unexpected BDCMF content category '[*ContentCategory*]'

This message indicates that the image does not include movie content. Therefore, it is expected that `ContentCategory="BD-ROM Data Media"` and `CMFType="P"`. This message indicates that the `ContentCategory` attribute contains another value.

First Playback is a BD-J Title

This message indicates that the FirstPlayback Title was identified as a BD-J Title but the BDCMF information for the same Title does not indicate that it is a BD-J Title.

The `TitleInfo` element includes the one child element `ContentInfo` for each Title. The `ContentInfo` element includes two attributes which indicate if the Title is a BD-Live and/or BD-J Title. During the analysis, the EclipseSuite tools determine the type of content of each Title and compare this back to the `TitleInfo` in the BDCMF. This condition occurs when there are differences.

TopMenu is a BD-J Title

This message indicates that the TopMenu Title was identified as a BD-J Title but the BDCMF information for the same Title does not indicate that it is a BD-J Title.

The `TitleInfo` element includes the one child element `ContentInfo` for each Title. The `ContentInfo` element includes two attributes which indicate if the Title is a BD-Live and/or BD-J Title. During the analysis, the EclipseSuite tools determine the type of content of each Title and compare this back to the `TitleInfo` in the BDCMF. This condition occurs when there are differences.

Title (*Title#*) is a BD-J Title

This message indicates that a Title was identified as a BD-J Title but the BDCMF information for the same Title does not indicate that it is a BD-J Title.

The `TitleInfo` element includes the one child element `ContentInfo` for each Title. The `ContentInfo` element includes two attributes which indicate if the Title is a BD-Live and/or BD-J Title. During the analysis, the EclipseSuite tools determine the type of content of each Title and compare this back to the `TitleInfo` in the BDCMF. This condition occurs when there are differences.

Severity

This rule is triggered when the content of an image does not match the description given by the BDCMF.CMF file. It is likely that the BDCMF.CMF file is incorrect. However, the fields in the BDCMF.CMF file describing the image determine how the image will be processed. It is unknown how these conditions may affect processing of the image. Therefore, this rule is considered a WARNING.

> **NOTE**
> *If you find that these conditions do cause other errors then you may need to upgrade the severity of this rule to an* ERROR.

Cause

This problem is caused by the authoring system or utility that last updated the BDCMF file set.

Solution

The solution to this problem depends on the actual condition that triggered it. Contact Eclipse Customer Support for assistance.

Type:	Blu-ray
Reference:	BDCMF Specifications
Default Program Action:	Warning

Rule ID: 1520

BDCMF Bus Encryption Flag Mismatch

The Bus Encryption Flag specified in the BDCMF does not match with the Bus Encryption Enabled flag in the Content Certificate.

Background

Bus encryption is another level of data protection. When enabled, it indicates that audio/video data being transferred between a drive and host PC should be encrypted.

Bus encryption is specified in the User Control Data (Bus Encryption Flag - BEF) and Content Certificate (Bus Encryption Enable - BEE). On a BDCMF image, the BEF flag can also be specified in the BDCMF.CMF file (BDCMF 1.10 or later). This rule is triggered when the BEE flag in the Content Certificate file of the BDCMF image and BEF flag in the BDCMF.CMF file don't agree.

Additional Info

When this rule is triggered, the **Additional Info** column in the analysis will display the following message.

BDCMF: [*Enabled/Disabled*], CC: [*Enabled/Disabled*]

This message indicates one of the following conditions:

- *The BDCMF BEF flag is set but the BEE flag in the Content Certificate is not.*
- *The BDCMF BEF flag is not set but the BEE flag in the Content Certificate is set.*

Severity

This condition is considered a warning since the BEF flag in the BDCMF does not determine if bus encryption will be set on discs produced from the image. The bus encryption flags in the User Control Data (UCD) and Content Certificate (CC) are the true indicators whether the discs will contain bus encryption. If there are any inconsistencies within the UCD and CC, then other errors will be triggered.

Cause

This problem is typically caused by the authoring application.

Solution

It is possible that this condition may be corrected if the image is processed using ImageCopy. ImageCopy will set the bus encryption flag in the BDCMF to match that of the UCD and CC. To confirm, analyze the output image and ensure the error no longer occurs. Otherwise, the image may need to be re-authored. Contact Eclipse Support for further assistance.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Warning

Rule ID: 1673

BDCMF Clip Encryption status does not match CPS Unit

The encryption status of a Clip AV file (*.m2ts) does not match with the encryption status of the CPS Unit that is assigned to it.

Background

The BDCMF specifications include the "Encryption" attribute in each Clip AV File entry, which is used to specify whether the Clip AV file is encrypted.

During analysis of a BD image, the EclipseSuite tools map the relationship between CPS Units and Clip AV Stream Files. A CPS Unit refers to a group of Titles that are encrypted with the same Title Key. Titles contain references to other objects which eventually refer to Clip AV files. Therefore, a Clip AV file will always map to a specific CPS Unit.

For every CPS Unit there is an associated CPS Unit Usage File (CPSUnitXXXXX.cci, where XXXXX is the CPS Unit number to which the CPS Unit Usage file is associated). The CPS Unit Usage File includes Copy Control Information (CCI) which is used to specify the encryption status of the CPS Unit and all the Titles within the same CPS Unit. The encryption status of all Clip AV files in the same CPS Unit must be the same as the encryption status of the CPS Unit.

Once it is determined which CPS Unit number is assigned to a Clip AV Stream file, the EclipseSuite tools will confirm that the encryption status of the Clip and the CPS Unit match. Otherwise, this rule is triggered.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display more details with the following message.

Clip [*####.m2ts*] [*EncryptionStatus*]**, CPSUnit(#####)** [*EncryptionStatus*]

This message identifies the Clip file, CPS Unit and their encryption status of each.

The encryption status of the Clip file is determined by the Copy Permission Indicator bits in the first Aligned Unit of the file. The encryption status of the CPS Unit is determined by the CCI bits in the associated CPS Unit Usage File.

If the copy protection status does not match between the CPS Unit and Clip AV file, then it may lead to playability problems.

Severity

This rule is considered an ERROR since inconsistencies in the encryption status of CPS Units and Clip files is known to cause playability problems.

Cause

This problem is caused by the authoring system that created the image.

Solution

Contact Eclipse Customer Support for further assistance.

Type:	Blu-ray
Reference:	BDCMF Specifications
Default Program Action:	Error

Rule ID: 1542

BDCMF CPType attribute missing

The CPType attribute, which specifies the content protection system for a BDCMF image, is missing from the BDCMF.CMF file.

Background

`CPType` is an XML attribute for the `ContentProtection` element. When the `ContentProtection` element is specified, it indicates that the image is protected and the `BDType` attribute specifies whether it is protected with '`AACS`' or '`BDPlus`'.

Severity

This rule is considered an ERROR since the image may not be able to be processes if the type of copy protection is not known.

Cause

The CPType attribute is typically set during authoring. Therefore, this would indicate an authoring problem.

Solution

Since there are only two possible values for this attribute, it may be easy to edit the BDCMF.CMF file if the protection type is known. The BDCMF file is an XML (text) file. However, you must be familiar with the structure of this file and with the BDCMF specifications before making any changes. If manual editing of the image is not possible, then it must be returned to authoring.

Type:	Blu-ray
Reference:	BDCMF Specifications
Default Program Action:	Error

Rule ID: 1405

BDCMF Distributor

This is an informational message that identifies the Distributor of the Blu-ray Video Movie.

Background

The '`Distributor`' is a field in the BDCMF 1.03 specifications and it is used by authoring systems to identify a BD movie's distributor. If specified in the BDCMF.CMF file, the Distributor name will be displayed in the Additional Info column of the Analysis.

Type:	Blu-ray
Reference:	BDCMF 1.03 Specifications
Default Program Action:	Info

Rule ID: 1622

BDCMF File attribute missing or incorrect

An XML element attribute is missing or contains an invalid value.

Background

The BDCMF specifications require certain elements and attributes in the files which make part of the file-set for a Blu-ray Video image. During analysis, the EclipseSuite tools validate the elements and their attributes to make sure they are correct. Some elements and/or attributes are required in the encryption of a BDCMF image. Therefore, if any of these elements or attributes are missing or if they contain an invalid value, it is possible that it may cause the analysis or encryption process to abort.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display more details as to the cause of this error.

The conditions described below refer to the files KEY.DAT, FAI.DAT and AACS1.DAT.

KEY.DAT: no keys found!

This message indicates that the '`NumOfCPSUnit`' attribute in the KEY.DAT file is missing or has an invalid value. This attribute specifies the number of CPS Units in the image and must match the number of CPS Units that is specified in the BDCMF.CMF file. This attribute is for the `CPSUnitInfo` element which also includes child elements that describe the CPS Unit Key value that is used to encrypt the user data. If the '`NumOfCPSUnit`' attribute is missing or contains an invalid value, then it is assumed that no CPS Units exist, which, for a Blu-ray Video image is invalid.

KEY.DAT: ExistenceOnDisc entry missing for CPS Unit index [*CPSUnitNumber*]

This message indicates that the '`ExistenceOnDisc`' attribute for one of the '`CPSUnit`' elements in the KEY.DAT file is missing. This attribute is used to specify whether the CPS Unit key is stored in the CPS Unit Key file on the BD-ROM disc or if the key is created for downloading purposes only and not stored in the CPS Unit Key file on the BD-ROM disc. The BDCMF specifications require that this attribute be specified.

KEY.DAT: Key not found for CPS Unit index [*CPSUnitNumber*]

This message indicates that the '`CPSUnitKeyValue`' attribute for one of the '`CPSUnit`' elements in the KEY.DAT file is missing. The value of this attribute is the CPS Unit key that is used for encryption. Without it, the user data cannot be encrypted. The BDCMF specifications require that this attribute be specified.

KEY.DAT: Could not find entries for CPS Unit index [*CPSUnitNumber*]

This message indicates that the '`CPSUnitNo`' attribute for one of the '`CPSUnit`' elements in the KEY.DAT file is missing. This attribute is used to specify the encryption key for a CPS Unit. The CPS Unit number identifies the encryption key that will be used to encrypt Clip AV stream files that are assigned to the same CPS Unit number.

File [**.m2ts*] **expected size attribute** [*size*] **Bytes**

This message indicates that the `Size` attribute for a Clip AV stream file is missing. Each Clip AV Stream file is described with a `<File>` element in the AACS1.DAT or FAI.DAT files. Each `<File>` element includes a `Size` attribute which specifies the file's size in bytes. This message indicates that the `Size` attribute is missing.

Note: *When using BDCMF 0.90, this condition refers to Clip AV File entries in the AACS1.DAT file. The Clip AV File entries are used on a Type A image during the encryption process. Therefore, if this condition occurs on a Type B or later, then it can be ignored.*

Severity

This rule is considered an ERROR since all conditions that trigger it are serious.

Note: *The last condition having to do with the expected size attribute may not affect the Eclipse software if the image uses BDCMF 0.90 or earlier. However, if this image is to be processed with non-Eclipse software, it should be considered serious.*

Cause

The KEY.DAT file is created during the encryption process. Therefore, for the above conditions having to do with the KEY.DAT file, the cause is typically the utility that encrypted the image.

For the above condition having to do with the expected size atttribute, the cause if normally the authoring system that created the image.

Solution

Contact Eclipse Support for the above conditions having to do with the KEY.DAT file. For the last condition having to do with the expected size attribute, it may be ignored as long as you are using Eclipse software to process the image and don't plan to send the image elsewhere for processing.

Type:	Blu-ray
Reference:	BDCMF Specifications 0.90 to 1.0x
Default Program Action:	Error

Rule ID: 1595

BDCMF File Missing

The Blu-ray image is missing a required BDCMF file.

Background

The Blu-ray Disc Cutting Master Format (BDCMF) is a standardized method of storing and interchanging BD-ROM contents. This standard is part of the Blu-ray Disc Read-Only Format Part 2: File System Specifications and is detailed System Description BDCMF version 1.01.

The following files are required for all image types as of BDCMF version 1.01:

Required Files	Optional Files	Required Files for Type A w/ Partial Info
BDCMF.CMF	PACL1.DAT	UKF.DAT
UD.DAT	BCA.DAT	ODOFL0.DAT
UCD.DAT	DAL0.DAT	RPC-BDCMF.CMF
PIC.DAT	DAL1.DAT	ODFL1.DAT (Mandatory for DL)
PACL0.DAT		SKF.DAT (Mandatory when Sequence Keys is used)
FAI.DAT		File Address Information

NOTE
Previous versions of BDCMF and certain image types may mandate alternative files.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will identify the missing file with one of the following messages.

Order Delivery File Data

The Order Delivery file (ODFL0.DAT) is missing the Content Certificate data. This file is a copy of the order file received from AACS LA. It contains the signed certificate that was used to sign the image.

Order Delivery File

The Order Delivery File (ODFL0.DAT) for layer 0 is missing. This file is a copy of the order file received from AACS LA. It contains the signed certificate that was used to sign the image.

Layer 1 Order Delivery File

The Order Delivery File (ODFL1.DAT) for layer 1 is missing. This file is a copy of the order file received from AACS LA. It contains the signed certificate that was used to sign the image.

File [*Filename*] expected size attribute [*Size*] Bytes. Clip entry could not be found

The FAI.DAT file includes a `<File>` entry for each Clip AV Stream file. Each entry specifies the address and size of a Clip AV file. This message indicates that the FAI.DAT file is missing the `<File>` entry for the file specified by this message.

The `<File>` entries in the FAI.DAT file are used by encryption tools during the image encryption process. If there are missing `<File>` entries, then the image may not be encrypted properly. ImageCopy does not use the Clip AV file information in the FAI.DAT. Instead, it parses the UDF file system of the image and builds its own list of Clip AV file entries. Therefore, if using ImageCopy, this condition may not have any effect. To confirm, run an analysis on the output image.

Severity

This condition is considered an ERROR because the Eclipse tools cannot proceed without the required file.

Cause

The Type A with Partial Information image did not get created properly.

Solution

The image should be re-created with all of the required files to correct this condition.

Type: Blu-ray
Reference: BDCMF Specifications version 1.01 Section 2.3 and 2.5
Default Program Action: Error

Rule ID: 1548

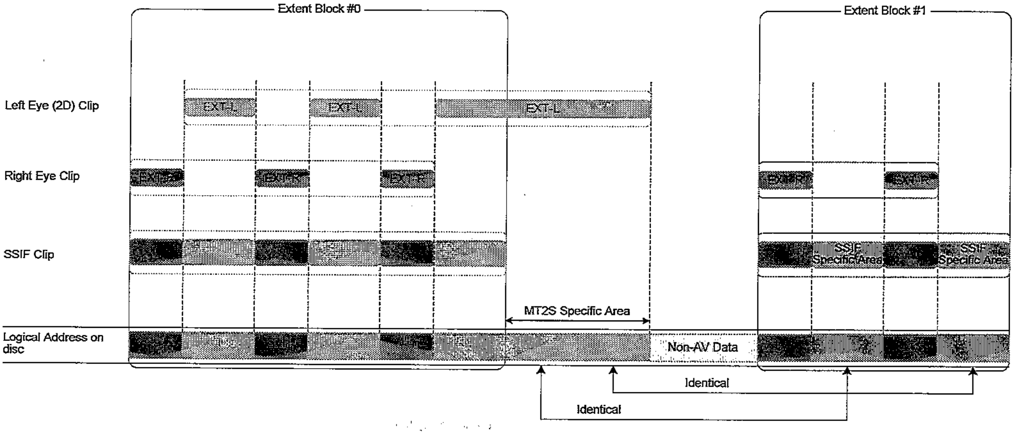
BDCMF M2TS and SSIF Specific Areas overlap

An extent from the M2TS Specific Area overlaps with another extent in the SSIF Specific Area.

Background

The Blu-ray 3D format includes an M2TS file for the left eye and another for the right eye. For conventional 2D Blu-ray video playback, only the data from the left eye is played. The 3D format also includes a Stereoscopic Interleaved File (SSIF), which consists of interleaved extents from the left and right eye files. The contents of the SSIF file are used for 3D playback.

The 3D format imposes a restriction on the size of extents. This restriction does not apply to 2D Clip extents. Therefore, when the left eye 2D M2TS file includes extents whose lengths exceeds the maximum allowed by the 3D specifications, the part of the extent that exceeds the maximum is duplicated in the SSIF file into one or more extents. The data areas (extents) that were duplicated are referred to as 'M2TS Specific Area' and 'SSIF Specific Area'. On a BDCMF image, the BDCMF specifications include sections that describe these areas. Each extent entry for the M2TS and SSIF Specific Areas include a start address and length. This error indicates that an extent in the M2TS Specific Area overlaps with another from the SSIF Specific Area.


Extent Block #0
Extent Block #1
Left Eye (2D) Clip
Right Eye Clip
SSIF Clip
Logical Address on disc
EXT-L
EXT-L
EXT-L
EXT-R
EXT-R
EXT-R
EXT-R
EXT-R
SSIF Specific Area
SSIF Specific Area
MT2S Specific Area
Non-AV Data
Identical
Identical

Severity

This condition indicates that an extent's start address or length is incorrect. Encryption tools, such as ImageCopy, use the extent information to know where encryption needs to be applied. This condition may cause encryption tools to fail. Therefore, this is considered an ERROR.

> **NOTE**
> *Although ImageCopy may trigger this rule during encryption, it is not affected by this condition. ImageCopy builds its own list of extents for each file from the UDF file system of the image and uses those instead. Therefore, if using Eclipse software to process an image with this condition, this rule can be IGNORED or set to INFO.*

Cause

This condition is caused by the authoring system that created the image.

Solution

The Eclipse software is not affected by this condition. However, if this image is to be processed with non-Eclipse software, then the image must be re-authored.

Type:	3D-BD
Reference:	BDCMF Specifications Version 1.21
Default Program Action:	Error

Rule ID: 1736

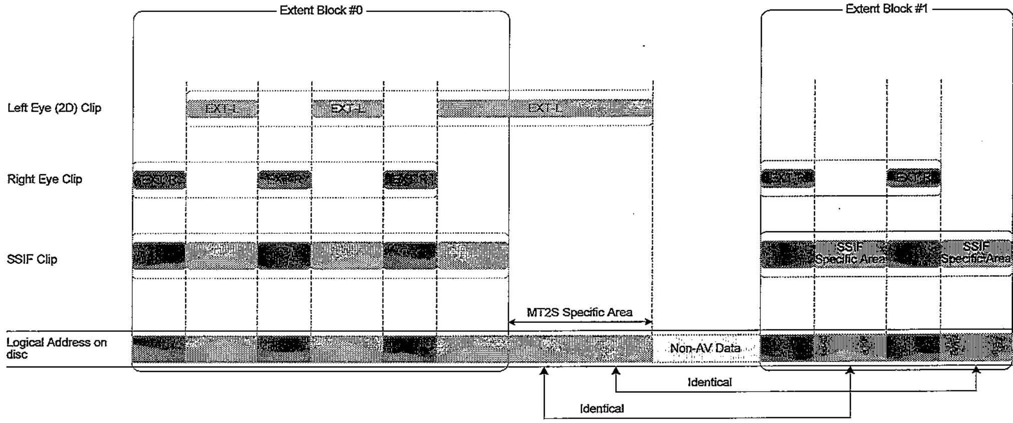
BDCMF M2TS Specific Areas overlap

The M2TS Specific Area extents in the BDCMF file overlap.

Background

The Blu-ray 3D format includes an M2TS file for the left eye and another for the right eye. For conventional 2D Blu-ray video playback, only the data from the left eye is played. The 3D format also includes a Stereoscopic Interleaved File (SSIF), which consists of interleaved extents from the left and right eye files. The contents of the SSIF file are used for 3D playback.

The 3D format imposes a restriction on the size of extents. This restriction does not apply to 2D Clip extents. Therefore, when the left eye 2D M2TS file includes extents whose lengths exceeds the maximum allowed by the 3D specifications, the part of the extent that exceeds the maximum is duplicated in the SSIF file into one or more extents. The data areas (extents) that were duplicated are referred to as 'M2TS Specific Area' and 'SSIF Specific Area'. On a BDCMF image, the BDCMF specifications include sections that describe these areas. Each extent entry for the M2TS and SSIF Specific Areas include a start address and length. This error indicates that two extents in the M2TS Specific Area overlap.


Extent Block #0
Extent Block #1
Left Eye (2D) Clip
Right Eye Clip
SSIF Clip
EXT-L
EXT-L
EXT-L
EXT-R
EXT-R
EXT-R
EXT-R
EXT-R
SSIF Specific Area
SSIF Specific Area
MT2S Specific Area
Logical Address on disc
Non-AV Data
Identical
Identical

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will identify the M2TS Clip file which includes the invalid extent.

[*Filename*], Start [*Start*] Size [*Size*]

This message identifies the file entry in the BDCMF which triggered this error. It refers to an extent in the M2TS Specific Area of the left eye (2D) Clip file. Since this extent is duplicated in the SSIF file, it is described in the File entries of the SSIF file.

At least one of the extents entries for the SSIF file includes sub-extent entries called '`SSIFSpecificArea`'. These entries are used to describe the extents that are duplicated between the M2TS and SSIF files. The `SSIFSpecificArea` entries include a `Start`, `Size` and `RefAreaStart` attributes. The Start attribute specifies the address of an extent in the SSIF file and the `RefAreaStart` attribute specifies the start address of an extent for the same data in the left eye (2D) Clip file.

This condition indicates that two extents specified by the `RefAreaStart` attributes overlap each other.

Example:

```
<File Type="ClipAVStream" Name="10001.ssif" Size="1234567890" Access="EXTENT">
    <CPSUnitNo>1</CPSUnitNo>
    <Encryption>Encrypted</Encryption>
    <Extent Start="nnnnnnn" Size="1234" />
    <Extent Start="nnnnnnn" Size="2345" >
    <SSIFSpecificArea Start="xxxxxx" Size="xxxx" RefAreaStart="xxxxx" />
    <SSIFSpecificArea Start="xxxxxx" Size="xxxx" RefAreaStart="xxxxx" />
    ...
    </Extent>
    ...
</File>
```

Severity

This condition indicates that an extent's start address or length is incorrect. Encryption tools, such as ImageCopy, use the extent information to know where encryption needs to be applied. This condition may cause encryption tools to fail. Therefore, this is considered an ERROR.

NOTE
Although ImageCopy may trigger this rule during encryption, it is not affected by this condition. ImageCopy builds its own list of extents for each file from the UDF file system of the image and uses those instead. Therefore, if using Eclipse software to process an image with this condition, this rule can be IGNORED or set to INFO.

Cause

This condition is caused by the authoring system that created the image.

Solution

The Eclipse software is not affected by this condition. However, if this image is to be processed with non-Eclipse software, then the image must be re-authored.

Type: 3D-BD
Reference: BDCMF Specifications Version 1.21
Default Program Action: Error

Rule ID: 1735

BDCMF missing L0 PAC data

The BDCMF.CMF file does not contain a reference to the element that describes the PACL0.DAT file.

Background

The PAC data files contain Physical Access Control information for BD25 media. The information is provided in the files PACL0.DAT and PACL1.DAT for layer 0 and layer 1, respectively. Only PACL0.DAT is required by the BDCMF specifications. It is possible that the file may be included with the image but it will be ignored if the BDCMF.CMF file does not include a reference to it.

Severity

This rule is considered an ERROR since this file is required by the Blu-ray and BDCMF specifications. Although analysis of the image may continue with this error, mastering may not be possible since the PACL0.DAT file is required.

Cause

This problem is typically caused by the authoring system that created the image.

Solution

It is possible that the reference to this file can be created manually if you are familiar with the structure of the BDCMF.CMF file. Contact Eclipse Support for assistance.

Type: Blu-ray
Reference: BDCMF Specifications
Default Program Action: Error

Rule ID: 1406

BDCMF missing User Control Data

The BDCMF.CMF file is missing a reference to the user control data file CONTROL.DAT.

Background

The user control data file CONTROL.DAT contains physical information for a BD9 media. It may also include additional AACS information if the image is protected with AACS. This file is described inside the BDCMF.CMF. This error indicates that the BDCMF.CMF is missing a reference to the CONTROL.DAT. However, since the Control data file is only required for BD9 media, it may not be a serious problem. It is possible that the file may be included with the image but it will be ignored if the BDCMF.CMF file does not include a reference to it.

Severity

This rule is considered a WARNING since the file is not required for most images. However, if the image is a BD9, then the file is required and this rule should be considered an ERROR.

NOTE
A BD9 is Blu-ray Video content on DVD media. This format is virtually non-existent and, therefore, unlikely that you will ever see it.

Cause

This problem typically is caused by the authoring system that created the image.

Solution

It is possible that the reference to this file can be created manually if you are familiar with the structure of the BDCMF.CMF file. Contact Eclipse Support for assistance.

Type:	Blu-ray
Reference:	BDCMF Specifications
Default Program Action:	Warning

Rule ID: 1407

BDCMF missing user data

The BDCMF.CMF file is missing a reference to the user data file UD.DAT.

Background

The BDCMF.CMF file is the primary file describing a Blu-ray image. It provides a description and references to the rest of the files in the CMF file set. The UD.DAT file contains the user data of the image and, therefore, it is required to be present. It is possible that the file may be included with the image but it will be ignored if the BDCMF.CMF file does not include a reference to it.

Severity

This rule is considered an ERROR since it is impossible to process this image without the user data file.

Cause

This problem is typically caused by the authoring system that created the image.

Solution

Since the reference information to this file is easy to determine, it is possible that this problem can be corrected by manually editing the BDCMF.CMF file. The reference can also be copied from a known good image then edited to match the current image. However, you must be familiar with the BDCMF specifications and know where the changes need to be made. Contact Eclipse Customer Support for further assistance.

Type:	Blu-ray
Reference:	BDCMF Specifications
Default Program Action:	Error

Rule ID: 1408

BDCMF option not supported

The EclipseSuite tools and BDCMF specifications do not support the use of Sequence Key Blocks.

Severity

This rule is considered an ERROR since it indicates that possibly the image was meant to support Sequence Key Blocks. Unfortunately, the BDCMF version used does not support it.

Cause

This problem is typically caused by the authoring system that created the image.

Solution

The image must be re-authored with the correct version of BDCMF that supports Sequence Key Blocks.

Type:	Blu-ray
Reference:	BDCMF Specifications
Default Program Action:	Error

Rule ID: 1476

BDCMF Region

This rule identifies the control status of each Region of a BDCMF image.

BDCMF defines the regions A, B and C. Each can have one of the following attributes:

Allowed - The entire disc can be played back.
Limited - Only a part of the disc can be played back.
Prohibited - The entire disc can't be played back.
Not Applicable - The authoring studio cannot set Region.

When this rule is triggered, the **Additional Info** column in the Analysis will display each region with one of the above attributes.

Type: Blu-ray
Reference: BDCMF Specifications
Default Program Action: Info

Rule ID: 1477

BDCMF required Element or Attribute missing

This is a generic error that occurs when a required XML element or attribute is missing in a file that is part of the BDCMF file set.

Background

Many of the BDCMF elements or attributes are provided for informational purposes only and, therefore, do not affect in the processing of a Blu-ray image. However, there are some that are critical. If any critical element or attribute is missing, you will normally see other related errors. If you only see this error, then it is likely that the image will be processed without problem.

> **NOTE**
> *If an element or attribute that does not affect processing of the image is missing, the EclipseSuite tools will continue despite the error. Other utilities many not be as forgiving.*

Type: Blu-Ray
Reference: BDCMF Specifications
Default Program Action: Error

Rule ID: 891

BDCMF Revision

This is an informational message that identifies the BDCMF Revision. The BDCMF Revision is used together with the VISAN number to create a unique identifier for a BDCMF image.

Type: Blu-ray
Reference: BDCMF Specifications
Default Program Action: Flag

Rule ID: 1616

BDCMF SSIF Specific Area off UDF Extent limits

One of the SSIFSpecificArea extents has an invalid length and/or start address.

Background

The 3D format includes Stereoscopic Interleaved files (*.SSIF) which are described in the BDCMF.CMF file. As with traditional Blu-ray stream files, all extents of each SSIF stream file are specified in the BDCMF file. The extents are the same as the ones specified in the UDF file system of the image. This error indicates that one of the extent entries in the BDCMF file is outside the UDF file system.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will identify the Clip AV Stream file which includes the invalid extent.

[*Filename*], **Start** [*Start*] **Size** [*Size*]

This message identifies the file entry in the BDCMF which triggered this error. The BDCMF file includes all the extents for this file. Since it is an SSIF file, at least one of the extents includes sub-extent entries called '`SSIFSpecificArea`'. *Similar to a normal* Extent *entry, the* `SSIFSpecificArea` *entries include a start and size attribute. One of these entries either starts outside the UDF file system or its size is too large that it falls outside the UDF file system.*

Example:

```
<File Type="ClipAVStream" Name="10001.ssif" Size="1234567890" Access="EXTENT">
    <CPSUnitNo>1</CPSUnitNo>
    <Encryption>Encrypted</Encryption>
    <Extent Start="nnnnnnn" Size="1234" />
    <Extent Start="nnnnnnn" Size="2345" >
    <SSIFSpecificArea Start="xxxxxx" Size="xxxx" RefAreaStart="xxxxx" />
    <SSIFSpecificArea Start="xxxxxx" Size="xxxx" RefAreaStart="xxxxx" />
    ...
    </Extent>
    ...
</File>
```

Severity

This condition is considered an ERROR since it may cause problems when processing the image.

Cause

This problem is normally caused by the authoring system that created the image. However, since the 3D format is quite new, it may be possible that the BDCMF file was edited manually and this condition may have been introduced during this process.

Solution

It may be possible to correct this condition by locating the Extent entry that triggered this error. The UDF information in the Eclipse analysis can be used to determine the correct extent start and length. Contact Eclipse Support for further assistance.

Type:	3D-BD
Reference:	Blu-ray 3D Specifications
Default Program Action:	Error

Rule ID: 1728

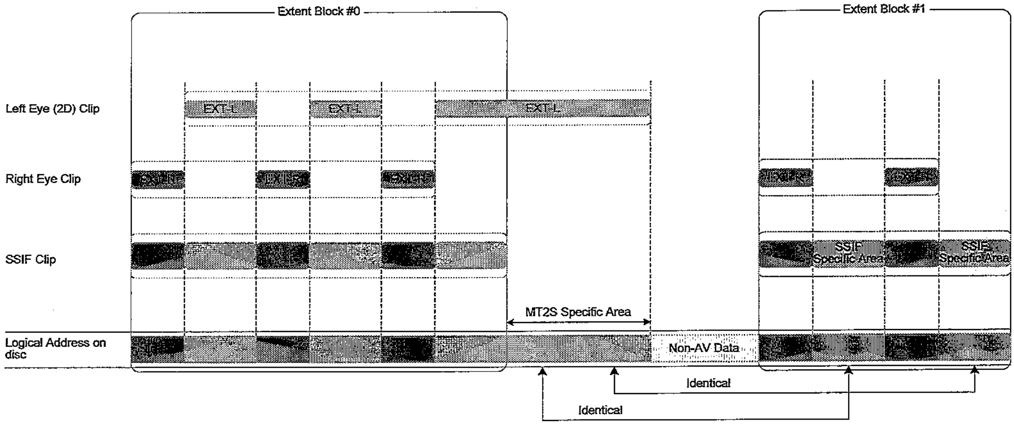
BDCMF SSIF Specific Areas overlap

The SSIF Specific Area extents in the BDCMF file overlap.

Background

The Blu-ray 3D format includes an M2TS file for the left eye and another for the right eye. For conventional 2D Blu-ray video playback, only the data from the left eye is played. The 3D format also includes a Stereoscopic Interleaved File (SSIF), which consists of interleaved extents from the left and right eye files. The contents of the SSIF file are used for 3D playback.

The 3D format imposes a restriction on the size of extents. This restriction does not apply to 2D Clip extents. Therefore, when the left eye 2D M2TS file includes extents whose lengths exceeds the maximum allowed by the 3D specifications, the part of the extent that exceeds the maximum is duplicated in the SSIF file into one or more extents. The data areas (extents) that were duplicated are referred to as 'M2TS Specific Area' and 'SSIF Specific Area'. On a BDCMF image, the BDCMF specifications include sections that describe these areas. Each extent entry for the M2TS and SSIF Specific Areas include a start address and length. This error indicates that two extents in the SSIF Specific Area overlap with one another.


Extent Block #0
Extent Block #1
Left Eye (2D) Clip
Right Eye Clip
SSIF Clip
Logical Address on disc
EXT-L
EXT-L
EXT-L
EXT-R
EXT-R
EXT-R
EXT-R
EXT-R
SSIF Specific Area
SSIF Specific Area
MT2S Specific Area
Non-AV Data
Identical
Identical

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will identify the SSIF file which includes the extents that overlap.

[#####.*ssif*], Start [*Start*] Size [*Size*]

This message identifies the SSIF file entry in the BDCMF which triggered this error. The BDCMF file includes all the extents for this file. Since it is an SSIF file, at least one of the extents includes sub-extent entries called `'SSIFSpecificArea'`*. Similar to a normal* Extent *entry, the* `SSIFSpecificArea` *entries include a start and size attribute. One of these entries is overlapping another and is triggering this condition.*

Example:

```
<File Type="ClipAVStream" Name="10001.ssif" Size="1234567890" Access="EXTENT">
    <CPSUnitNo>1</CPSUnitNo>
    <Encryption>Encrypted</Encryption>
    <Extent Start="nnnnnnn" Size="1234" />
    <Extent Start="nnnnnnn" Size="2345" >
    <SSIFSpecificArea Start="xxxxxx" Size="xxxx" RefAreaStart="xxxxx" />
    <SSIFSpecificArea Start="xxxxxx" Size="xxxx" RefAreaStart="xxxxx" />
    ...
    </Extent>
```

```
...
</File>
```

Severity

This condition indicates that an extent's start address or length is incorrect. Encryption tools, such as ImageCopy, use the extent information to know where encryption needs to be applied. This condition may cause encryption tools to fail. Therefore, this is considered an ERROR.

> **NOTE**
> *Although ImageCopy may trigger this rule during encryption, it is not affected by this condition. ImageCopy builds its own list of extents for each file from the UDF file system of the image and uses those instead. Therefore, if using Eclipse software to process an image with this condition, this rule can be IGNORED or set to INFO.*

Cause

This condition is caused by the authoring system that created the image.

Solution

The Eclipse software is not affected by this condition. However, if this image is to be processed with non-Eclipse software, then the image must be re-authored.

Type:	3D-BD
Reference:	Blu-ray 3D Specifications
Default Program Action:	Error

Rule ID: 1727

BDCMF subfolder not found

The explanation for this title check rule contains confidential information. Please refer to the studio-specific supplemental rules help PDF document. The document is available from Eclipse Support.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

Rule ID: 1744

BDCMF Type

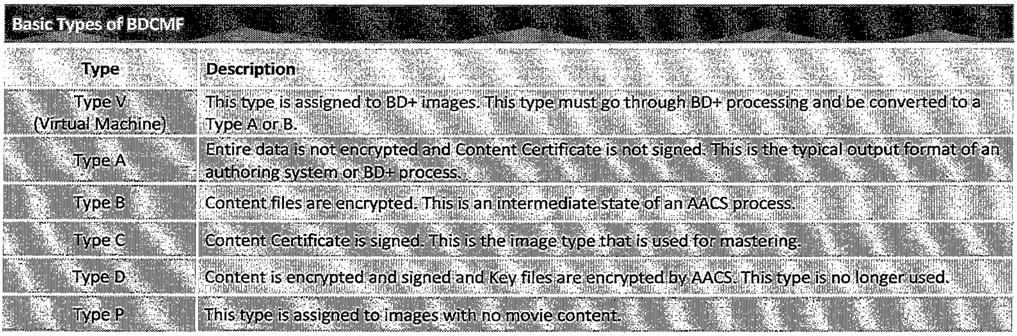
This is an informational message that identifies the process status of a BDCMF image.

Background

The BDCMF specifications assign a `Type` name to BDCMF images as they move through each process step.

During the various stages of BD processing, the `Type` name will change to reflect the current process status. This normally refers to the AACS encryption status of the image. The typical BDCMF Types are: A, B, C and D. However, there are some variations depending on the version of BDCMF.

The following picture describes BDCMF Types common to all versions of BDCMF:



Basic Types of BDCMF

Type	Description
Type V (Virtual Machine)	This type is assigned to BD+ images. This type must go through BD+ processing and be converted to a Type A or B.
Type A	Entire data is not encrypted and Content Certificate is not signed. This is the typical output format of an authoring system or BD+ process.
Type B	Content files are encrypted. This is an intermediate state of an AACS process.
Type C	Content Certificate is signed. This is the image type that is used for mastering.
Type D	Content is encrypted and signed and Key files are encrypted by AACS. This type is no longer used.
Type P	This type is assigned to images with no movie content.

Others

The BDCMF specifications also define two other, less common, BDCMF types: Type **AX** and **DK**.

- **Type AX** - This Type refers to the original Type A image but with Title Keys & Content Certificates. Once an image is processed up to a Type C (encrypted and signed), a Type AX can be created. This can be returned back to the customer. If the customer needs the image to be replicated again, the Type AX image can be re-submitted. The difference between submitting the Type A and Type AX for mastering is that the customer does not have to pay for AACS again.
- **Type DK** - Not currently used.

BDCMF 1.03

This version defines Type VU which is internal to the BD+ process. You should not see this in a pre-mastering or mastering process.

BDCMF 1.10

This version defines Types **BS** and **CS** (or Type B Secure and Type C Secure). The difference between these and the regular Type B and C is that the Title Keys are removed from the image and stored in an encrypted file. This secure file is created during the encryption process and becomes part of the BDCMF file set.

Additional Info

When this rule is triggered, **the Additional Info** column in the Analysis will identify the BDCMF Type. Note also that current versions of EclipseSuite will also display a separate message identifying the BDCMF Type. This way, users can flag any BDCMF Type if they wish to.

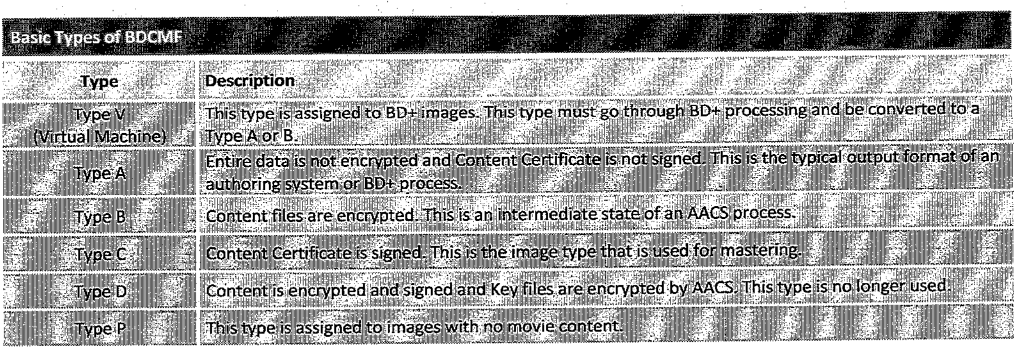
Type:	Blu-ray
Reference:	BDCMF Specifications
Default Program Action:	Info

Rule ID: 893

BDCMF Type A

This is an informational message that identifies a BDCMF Type A image.

A Type A image is a Blu-ray Video image which has not yet been encrypted. The following is a list of the most common BDCMF Types:



Basic Types of BDCMF

Type	Description
Type V (Virtual Machine)	This type is assigned to BD+ images. This type must go through BD+ processing and be converted to a Type A or B.
Type A	Entire data is not encrypted and Content Certificate is not signed. This is the typical output format of an authoring system or BD+ process.
Type B	Content files are encrypted. This is an intermediate state of an AACS process.
Type C	Content Certificate is signed. This is the image type that is used for mastering.
Type D	Content is encrypted and signed and Key files are encrypted by AACS. This type is no longer used.
Type P	This type is assigned to images with no movie content.

Type:	Blu-ray
Reference:	BDCMF Specifications
Default Program Action:	Info

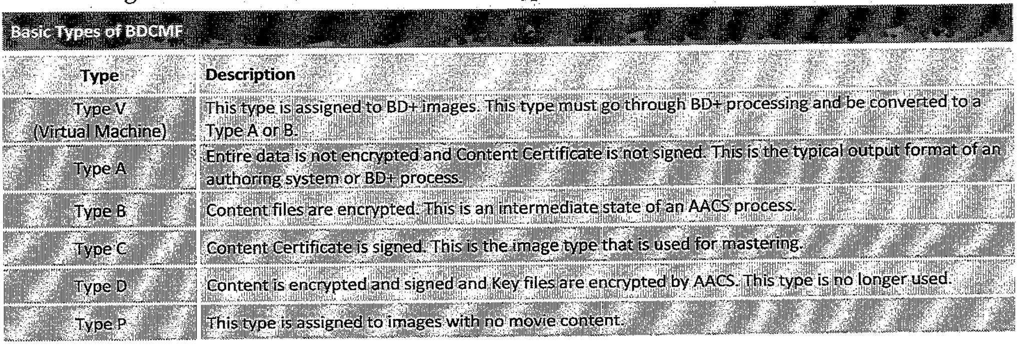
Rule ID: 1687

BDCMF Type AX

This is an informational message that identifies a BDCMF Type AX image.

A Type AX image is a Blu-ray Video image which has been previously mastered. Type AX includes the original unencrypted image with the Title Keys and Content Certificate that were used when the image was first mastered. This type of image is normally sent back to the customer so that they do not have to re-submit the CC's to AACS LA if the image is to be re-mastered in the future.

The following is a list of the most common BDCMF Types:



Basic Types of BDCMF

Type	Description
Type V (Virtual Machine)	This type is assigned to BD+ images. This type must go through BD+ processing and be converted to a Type A or B.
Type A	Entire data is not encrypted and Content Certificate is not signed. This is the typical output format of an authoring system or BD+ process.
Type B	Content files are encrypted. This is an intermediate state of an AACS process.
Type C	Content Certificate is signed. This is the image type that is used for mastering.
Type D	Content is encrypted and signed and Key files are encrypted by AACS. This type is no longer used.
Type P	This type is assigned to images with no movie content.

Type:	Blu-ray
Reference:	BDCMF Specifications
Default Program Action:	Info

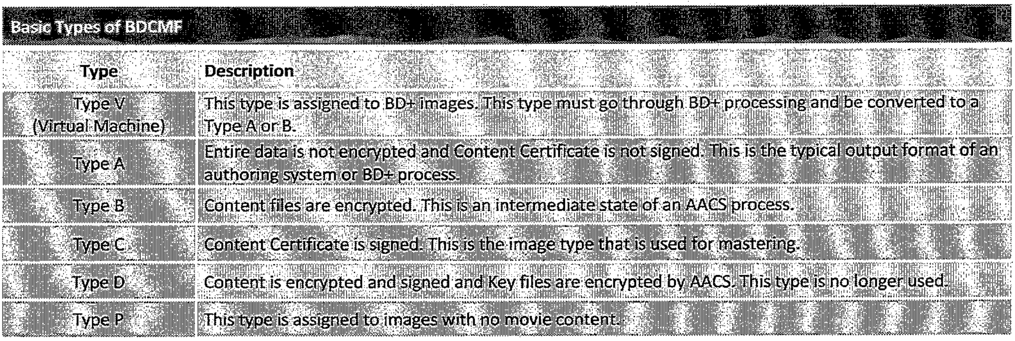
Rule ID: 1688

BDCMF Type B

This is an informational message that identifies a BDCMF Type B image.

A Type B image is a Blu-ray Video image which has been encrypted but has not been signed yet. This Type refers to an intermediate process step of a Blu-ray image. Type B images must be converted to Type C before they can be mastered.

The following is a list of the most common BDCMF Types:



Basic Types of BDCMF

Type	Description
Type V (Virtual Machine)	This type is assigned to BD+ images. This type must go through BD+ processing and be converted to a Type A or B.
Type A	Entire data is not encrypted and Content Certificate is not signed. This is the typical output format of an authoring system or BD+ process.
Type B	Content files are encrypted. This is an intermediate state of an AACS process.
Type C	Content Certificate is signed. This is the image type that is used for mastering.
Type D	Content is encrypted and signed and Key files are encrypted by AACS. This type is no longer used.
Type P	This type is assigned to images with no movie content.

Type:	Blu-ray
Reference:	BDCMF Specifications
Default Program Action:	Info

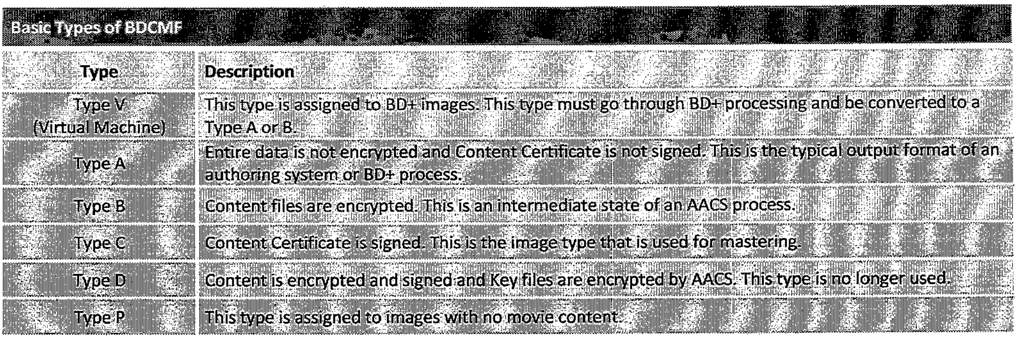
Rule ID: 1689

BDCMF Type BS

This is an informational message that identifies a BDCMF Type B Secure image (BS).

A Type BS image is a Blu-ray Video image which has been encrypted but has not been signed yet. A Type BS differs from a normal Type B in that the Title Keys that were used to encrypt the content are removed from the image and stored in a separate secure file. Just like a Type B image, a Type BS refers to an intermediate process step of a Blu-ray image. Type BS images must be converted to Type C or CS before they can be mastered.

The following is a list of the most common BDCMF Types:



Basic Types of BDCMF

Type	Description
Type V (Virtual Machine)	This type is assigned to BD+ images. This type must go through BD+ processing and be converted to a Type A or B.
Type A	Entire data is not encrypted and Content Certificate is not signed. This is the typical output format of an authoring system or BD+ process.
Type B	Content files are encrypted. This is an intermediate state of an AACS process.
Type C	Content Certificate is signed. This is the image type that is used for mastering.
Type D	Content is encrypted and signed and Key files are encrypted by AACS. This type is no longer used.
Type P	This type is assigned to images with no movie content.

Type: Blu-ray
Reference: BDCMF Specifications
Default Program Action: Info

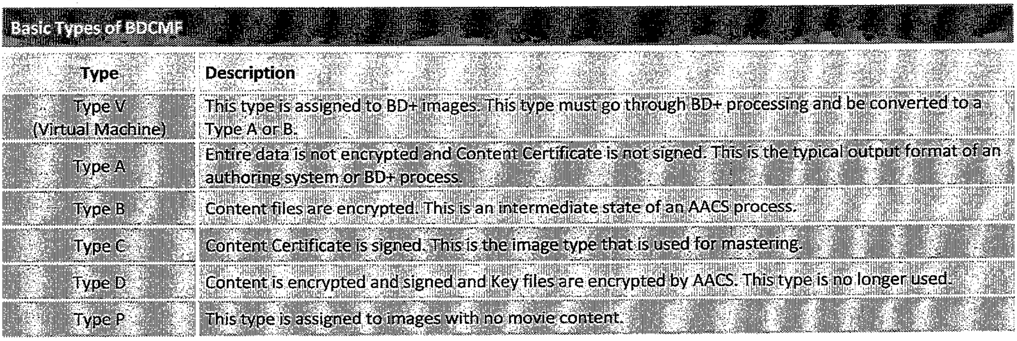
Rule ID: 1695

BDCMF Type C

This is an informational message that identifies a BDCMF Type C image.

A Type C image is a Blu-ray Video image which has been encrypted and signed. Type C images are ready to be mastered.

The following is a list of the most common BDCMF Types:



Basic Types of BDCMF

Type	Description
Type V (Virtual Machine)	This type is assigned to BD+ images. This type must go through BD+ processing and be converted to a Type A or B.
Type A	Entire data is not encrypted and Content Certificate is not signed. This is the typical output format of an authoring system or BD+ process.
Type B	Content files are encrypted. This is an intermediate state of an AACS process.
Type C	Content Certificate is signed. This is the image type that is used for mastering.
Type D	Content is encrypted and signed and Key files are encrypted by AACS. This type is no longer used.
Type P	This type is assigned to images with no movie content.

Type: Blu-ray
Reference: BDCMF Specifications
Default Program Action: Info

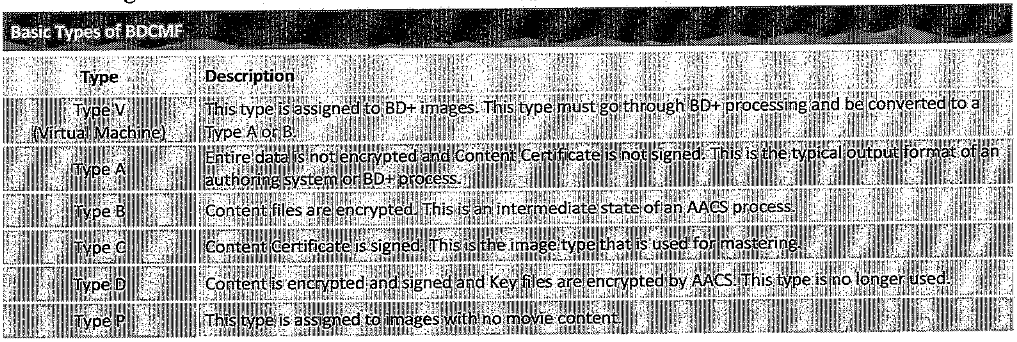
Rule ID: 1690

BDCMF Type C1

This is an informational message that identifies a BDCMF Type C1 image.

A Type C1 was defined in an intermediate BDCMF revision. It is basically the same as a normal Type C, which describes a BDCMF image which has been encrypted and signed. Type C1 images are ready to be mastered.

The following is a list of the most common BDCMF Types:



Basic Types of BDCMF

Type	Description
Type V (Virtual Machine)	This type is assigned to BD+ images. This type must go through BD+ processing and be converted to a Type A or B.
Type A	Entire data is not encrypted and Content Certificate is not signed. This is the typical output format of an authoring system or BD+ process.
Type B	Content files are encrypted. This is an intermediate state of an AACS process.
Type C	Content Certificate is signed. This is the image type that is used for mastering.
Type D	Content is encrypted and signed and Key files are encrypted by AACS. This type is no longer used.
Type P	This type is assigned to images with no movie content.

Type:	Blu-ray
Reference:	BDCMF Specifications
Default Program Action:	Info

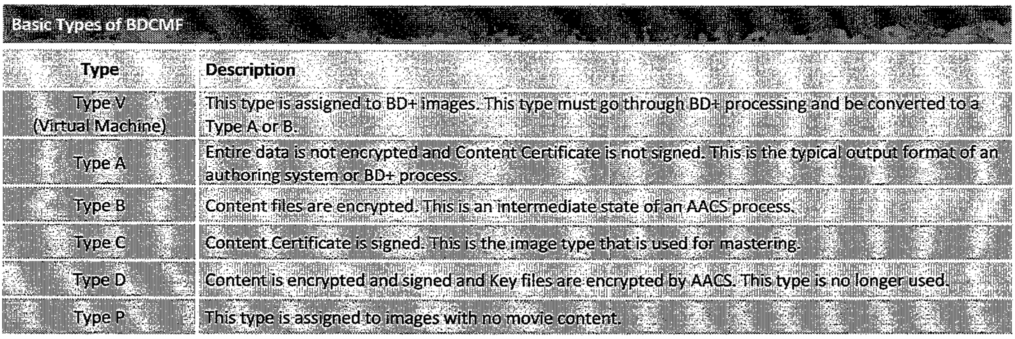
Rule ID: 1691

BDCMF Type C2

This is an informational message that identifies a BDCMF Type C2 image.

A Type C2 was defined in an intermediate BDCMF revision. It is basically the same as a normal Type C, which describes a Blu-ray Video image which has been encrypted and signed. However, Type C2 images also include MKB/SKB information. Type C2 images are ready to be mastered.

The following is a list of the most common BDCMF Types:



Basic Types of BDCMF

Type	Description
Type V (Virtual Machine)	This type is assigned to BD+ images. This type must go through BD+ processing and be converted to a Type A or B.
Type A	Entire data is not encrypted and Content Certificate is not signed. This is the typical output format of an authoring system or BD+ process.
Type B	Content files are encrypted. This is an intermediate state of an AACS process.
Type C	Content Certificate is signed. This is the image type that is used for mastering.
Type D	Content is encrypted and signed and Key files are encrypted by AACS. This type is no longer used.
Type P	This type is assigned to images with no movie content.

Type: Blu-ray
Reference: N/A
Default Program Action: Info

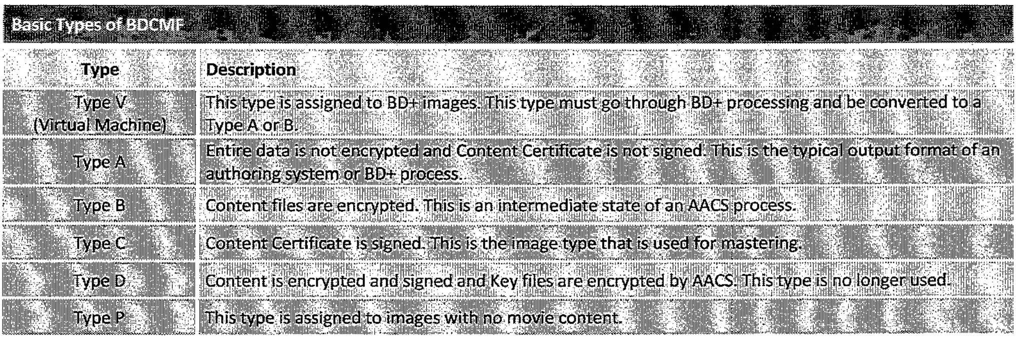
Rule ID: 1692

BDCMF Type CS

This is an informational message that identifies a BDCMF Type C Secure image (CS).

A Type CS image is a Blu-ray Video image which has been encrypted and signed. A Type CS differs from a normal Type C in that the Title Keys that were used to encrypt the content are also encrypted for security reasons. Just like a Type C image, a Type CS image is ready to be mastered.

The following is a list of the most common BDCMF Types:



Basic Types of BDCMF

Type	Description
Type V (Virtual Machine)	This type is assigned to BD+ images. This type must go through BD+ processing and be converted to a Type A or B.
Type A	Entire data is not encrypted and Content Certificate is not signed. This is the typical output format of an authoring system or BD+ process.
Type B	Content files are encrypted. This is an intermediate state of an AACS process.
Type C	Content Certificate is signed. This is the image type that is used for mastering.
Type D	Content is encrypted and signed and Key files are encrypted by AACS. This type is no longer used.
Type P	This type is assigned to images with no movie content.

Type: Blu-ray
Reference: BDCMF Specifications
Default Program Action: Info

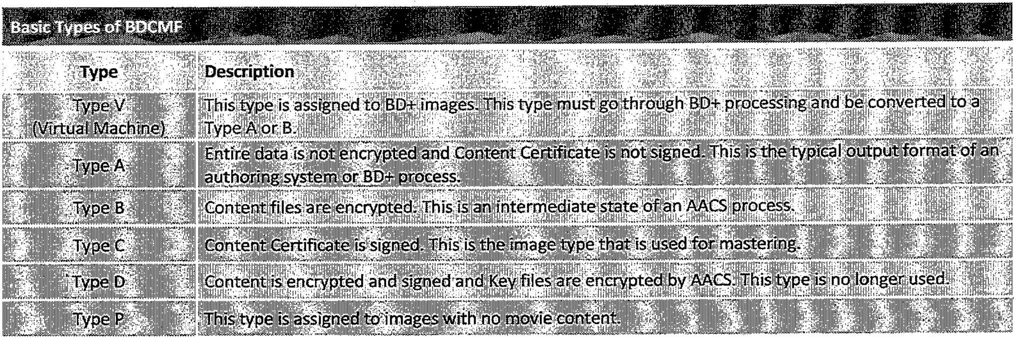
Rule ID: 1696

BDCMF Type D

This is an informational message that identifies a BDCMF Type D image.

A Type D image is a Blu-ray Video image which has been encrypted and signed. This Type normally exists in memory while a Type C is being mastered. The encoder system performs the last encryption steps converting the image to a Type D in memory. A Type D normally is not saved to hard disk.

The following is a list of the most common BDCMF Types:



Basic Types of BDCMF

Type	Description
Type V (Virtual Machine)	This type is assigned to BD+ images. This type must go through BD+ processing and be converted to a Type A or B.
Type A	Entire data is not encrypted and Content Certificate is not signed. This is the typical output format of an authoring system or BD+ process.
Type B	Content files are encrypted. This is an intermediate state of an AACS process.
Type C	Content Certificate is signed. This is the image type that is used for mastering.
Type D	Content is encrypted and signed and Key files are encrypted by AACS. This type is no longer used.
Type P	This type is assigned to images with no movie content.

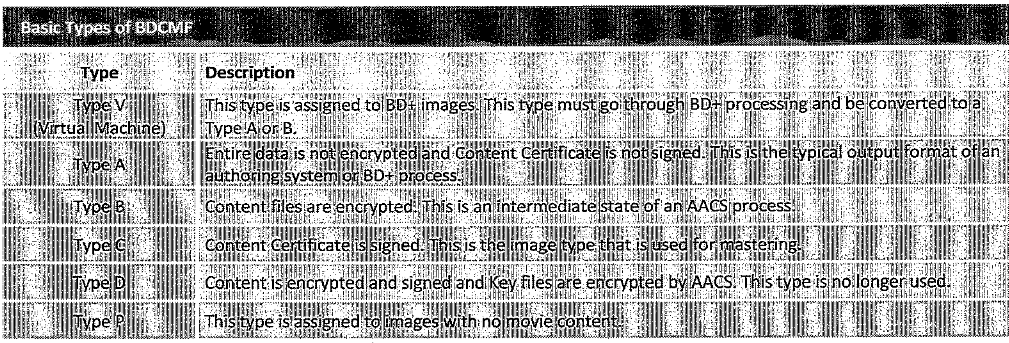
Type: Blu-ray
Reference: BDCMF Specifications
Default Program Action: Info

Rule ID: 1693

BDCMF Type DK

This is an informational message that identifies a BDCMF Type DK image. This Type was defined in an intermediate version of BDCMF specifications.

The following is a list of the most common BDCMF Types:



Basic Types of BDCMF

Type	Description
Type V (Virtual Machine)	This type is assigned to BD+ images. This type must go through BD+ processing and be converted to a Type A or B.
Type A	Entire data is not encrypted and Content Certificate is not signed. This is the typical output format of an authoring system or BD+ process.
Type B	Content files are encrypted. This is an intermediate state of an AACS process.
Type C	Content Certificate is signed. This is the image type that is used for mastering.
Type D	Content is encrypted and signed and Key files are encrypted by AACS. This type is no longer used.
Type P	This type is assigned to images with no movie content.

Type: Blu-ray
Reference: BDCMF Specifications
Default Program Action: Info

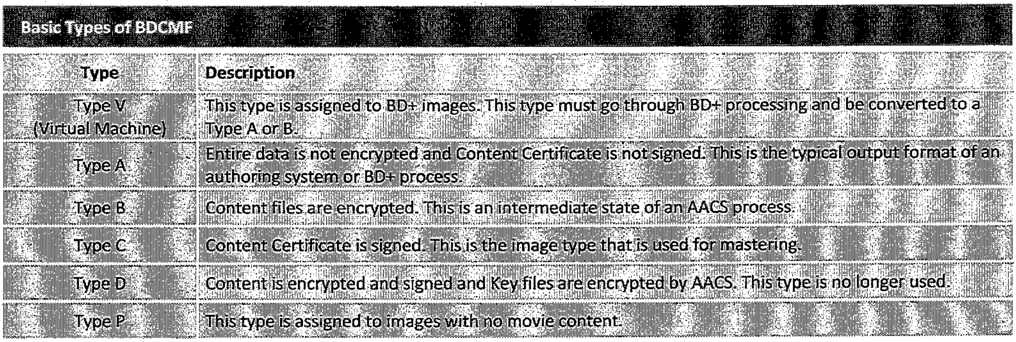
Rule ID: 1694

BDCMF Type P

This is an informational message that identifies a BDCMF Type P image.

A Type P describes a Blu-ray image that contains PC data (i.e. Not a Blu-ray Video). Type P images do not require any processing and are ready to be mastered.

The following is a list of the most common BDCMF Types:



Basic Types of BDCMF

Type	Description
Type V (Virtual Machine)	This type is assigned to BD+ images. This type must go through BD+ processing and be converted to a Type A or B.
Type A	Entire data is not encrypted and Content Certificate is not signed. This is the typical output format of an authoring system or BD+ process.
Type B	Content files are encrypted. This is an intermediate state of an AACS process.
Type C	Content Certificate is signed. This is the image type that is used for mastering.
Type D	Content is encrypted and signed and Key files are encrypted by AACS. This type is no longer used.
Type P	This type is assigned to images with no movie content.

Type: Blu-ray
Reference: BDCMF Specifications
Default Program Action: Info

Rule ID: 1686

BDCMF Type P TL

This is an informational message that identifies a Triple layer Blu-ray ROM BDCMF image.

Type: Exclude
Reference: None
Default Program Action: Info

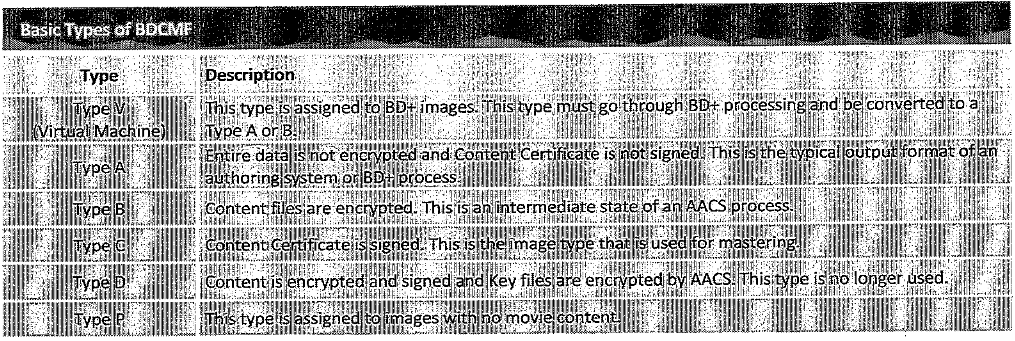
Rule ID: 1900

BDCMF Type V

This is an informational message that identifies a BDCMF Type V image.

A Type V describes a Blu-ray Video image which requires BD+ processing. A Type V image cannot be accepted for pre-mastering/mastering. When the BD+ process is applied to an image, the resulting image becomes a Type A, which is the typical image Type received in a pre-mastering process.

The following is a list of the most common BDCMF Types:



Basic Types of BDCMF

Type	Description
Type V (Virtual Machine)	This type is assigned to BD+ images. This type must go through BD+ processing and be converted to a Type A or B.
Type A	Entire data is not encrypted and Content Certificate is not signed. This is the typical output format of an authoring system or BD+ process.
Type B	Content files are encrypted. This is an intermediate state of an AACS process.
Type C	Content Certificate is signed. This is the image type that is used for mastering.
Type D	Content is encrypted and signed and Key files are encrypted by AACS. This type is no longer used.
Type P	This type is assigned to images with no movie content.

Type: Blu-ray
Reference: BDCMF Specifications
Default Program Action: Info

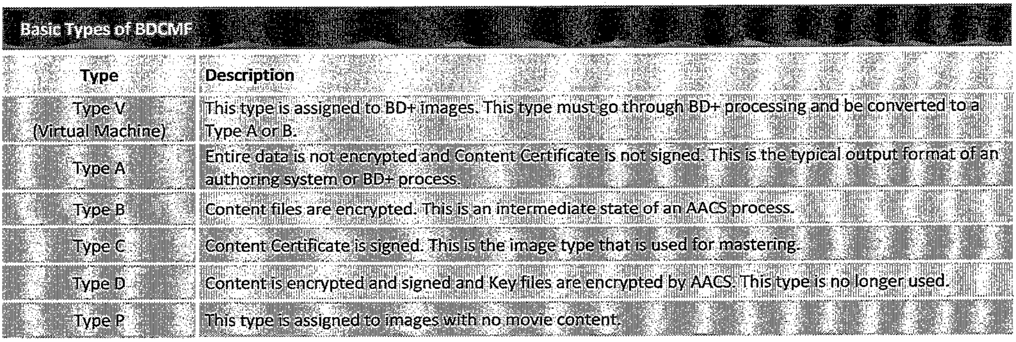
Rule ID: 1684

BDCMF Type VU

This is an informational message that identifies a BDCMF Type VU image.

A Type VU describes a Blu-ray Video image which requires BD+ processing but is in an intermediate stage. A Type VU image cannot be accepted for pre-mastering/mastering. When the complete BD+ process is applied to an image, the resulting image becomes a Type A, which is the typical image Type received in a pre-mastering process.

The following is a list of the most common BDCMF Types:



Basic Types of BDCMF

Type	Description
Type V (Virtual Machine)	This type is assigned to BD+ images. This type must go through BD+ processing and be converted to a Type A or B.
Type A	Entire data is not encrypted and Content Certificate is not signed. This is the typical output format of an authoring system or BD+ process.
Type B	Content files are encrypted. This is an intermediate state of an AACS process.
Type C	Content Certificate is signed. This is the image type that is used for mastering.
Type D	Content is encrypted and signed and Key files are encrypted by AACS. This type is no longer used.
Type P	This type is assigned to images with no movie content.

Type: Blu-ray

Reference: BDCMF Specifications
Default Program Action: Info

Rule ID: 1685

BDCMF Version

This is an informational message that identifies the version of the BDCMF image.

Type: Blu-ray
Reference: N/A
Default Program Action: Info

Rule ID: 1478

BDCMF Version 0.90

This is an informational message that identifies a Blu-ray image using BDCMF version 0.90.

Type: Blu-ray
Reference: BDCMF Specifications
Default Program Action: Info

Rule ID: 1697

BDCMF Version 0.9011

This is an informational rule that identifies an image using BDCMF version 0.9011.

Type: Exclude
Reference: N/A
Default Program Action: Info

Rule ID: 1789

BDCMF Version 0.97

This is an informational message that identifies a Blu-ray image using BDCMF version 0.97.

Type: Blu-ray
Reference: BDCMF Specifications
Default Program Action: Info

Rule ID: 1698

BDCMF Version 0.98

This is an informational message that identifies a Blu-ray image using BDCMF version 0.98.

Type:	Blu-ray
Reference:	BDCMF Specifications
Default Program Action:	Info

Rule ID: 1699

BDCMF Version 0.99

This is an informational message that identifies a Blu-ray image using BDCMF version 0.99.

Type:	Blu-ray
Reference:	BDCMF Specifications
Default Program Action:	Info

Rule ID: 1700

BDCMF Version 1.01

This is an informational message that identifies a Blu-ray image using BDCMF version 1.01.

Type:	Blu-ray
Reference:	BDCMF Specifications
Default Program Action:	Info

Rule ID: 1701

BDCMF Version 1.02

This is an informational message that identifies a Blu-ray image using BDCMF version 1.02.

Type:	Blu-ray
Reference:	BDCMF Specifications
Default Program Action:	Info

Rule ID: 1702

BDCMF Version 1.03

This is an informational message that identifies a Blu-ray image using BDCMF version 1.03.

Type:	Blu-ray
Reference:	BDCMF Specifications
Default Program Action:	Info

Rule ID: 1703

BDCMF Version 1.10

This is an informational message that identifies a Blu-ray image using BDCMF version 1.10.

Type: Blu-ray
Reference: BDCMF Specifications
Default Program Action: Info

Rule ID: 1704

BDCMF Version 1.19

This is an informational message that identifies a Blu-ray image using BDCMF version 1.19, which was an interim version that supported 3D.

Type: Exclude
Reference: BDCMF Specifications
Default Program Action: Info

Rule ID: 1776

BDCMF Version 1.20

This is an informational message that identifies a Blu-ray image using BDCMF version 1.20, which is the first official version supporting 3D.

Type: Exclude
Reference: BDCMF Specifications
Default Program Action: Info

Rule ID: 1810

BDCMF Version 1.21

This is an informational message that identifies a Blu-ray image using BDCMF version 1.21.

Type: Exclude
Reference: BDCMF Specifications
Default Program Action: Info

Rule ID: 1811

BDCMF VISAN Error

The VISAN number in the BDCMF.CMF file is invalid.

Background

In Blu-ray, an ISAN (International Standard Audiovisual Number) is a unique serial number required by

AACS as a content identifier. This number is stored in the Content ID field of the Managed Copy Manifest file (mcmf.xml). On a BDCMF image, this number is stored in the VISAN field of the BDCMF.CMF file.

On a disc, the Content ID number is used for copy management and online transactions. On a BDCMF image, the VISAN is provided for informational purposes and can be used to uniquely identify a BDCMF image.

During the analysis, the EclipseSuite tools compare the Content ID and VISAN values. This rule indicates that the two values did not match. The assumption is that the VISAN is invalid and the Content ID is correct. This is true unless the rule **ISAN Error** is triggered, which indicates that the Content ID ISAN value is incorrect.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display more details with one of the following messages.

BDCMF does not match Content ID ISAN. BDCMF VISAN: [*VISAN*]

This message indicates that the VISAN number in the BDCMF.CMF file does not match with the Content ID ISAN number that is stored in the Managed Copy Manifest File (mcmf.xml). The VISAN field should have the same value as the Content ID ISAN.

BDCMF VISAN Check digits are incorrect. Expected Digit1 (*CheckDigit1*), Digit2 (*CheckDigit2*)

The VISAN number has a specific structure where two of its digits are used to validate the rest of the number. The two check digits are determined by the rest of the VISAN number. The EclipseSuite tools recalculate the check digits then compare them to the check digits found in the VISAN from the BDCMF.CMF file.

Severity

The VISAN is present only in the BDCMF.CMF file and is provided for informational purposes. In some cases, this number can be used to uniquely identify the image. Therefore, this condition is considered only a WARNING.

Cause

The VISAN number is recorded in the BDCMF.CMF file by the authoring system.

Solution

Contact the author to confirm the correct VISAN number. Contact Eclipse Customer Support for further assistance.

Type:	Blu-ray
Reference:	BDCMF Specifications
Default Program Action:	Error

Rule ID: 1617

BDCMF XML file Load error

An error occurred while attempting to load and parse an XML file.

Background

The BDCMF specifications include the file BDCMF.CMF, which is the primary file describing a Blu-ray image. If the BDCMF version is 0.90 or earlier, then the file AACS1.DAT is also present. If the BDCMF version is 1.10 or later, then the file KEY.DAT file is present. These files are all formatted in XML. During analysis, these files are loaded into memory and their contents are parsed. In most cases, this error occurs due to invalid XML formatting such as a missing attribute, missing element or use of an illegal character. However, this can also be triggered by system errors.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display more details with one of the following messages.

KEY.DAT

The KEY.DAT file is a secure file that contains the keys that were used to encrypt the image. This file is created during the encryption of an image. In previous BDCMF versions, when an image was encrypted, the encryption keys were stored in the image itself unprotected. Starting with BDCMF 1.10, the encryption keys are removed from the image and stored in this highly secure file. The following conditions apply to this file only.

KEY.DAT: [*ErrorDescription*]. Line: [*LineNo*], Col: [*ColNo*]

This condition indicates that an error occurred while parsing the KEY.DAT file. It is likely that this was caused by an invalid character or formatting error. This message displays the error description and identifies the line and character position within the file where the error occurred. The error description should give you enough details as to the cause of the error.

KEY.DAT: Unknown parse Error - XML library reports no error!

This condition indicates that an unknown error occurred while parsing the KEY.DAT file. This condition may be caused by a system error. This condition may cause analysis of the image to fail.

Key.DAT file missing at least one required content category attribute

This condition indicates that the KEY.DAT file is missing a `ContentCategory` *attribute. This attribute identifies a Blu-ray image as 'BD-ROM Movie Media', 'BD-ROM Movie Media with BD DATA' or 'BD-ROM Data Media'. This attribute is required only when the image content is a 'BD-ROM Movie Media' or 'BD-ROM Movie Media with BD DATA'.*

KEY.DAT Missing VISAN and MasterID

The BDCMF Specifications require that at least the `VISAN` *or the* `MasterID` *be specified in the KEY.DAT file. The VISAN or MasterID are used for identification of a 'BD-ROM Movie Media'. The BDCMF 1.10 specifications require either one or both.*

KEY.DAT SAVE: [*Description*]. Line: [*LineNo*], Col: [*ColNo*]

This condition indicates an error while parsing the KEY.DAT file during a save operation. This message displays the error description and identifies the line and character position within the file where the error occurred. The error description should give you enough details as to the cause of the error.

BDCMF.CMF

This file is always present as it is the primary file describing a BDCMF image. This file describes some of the physical parameters of the final Blu-ray disc. It also describes the other files that are included as part of the BDCMF image. If the BDCMF version is after 0.90, then this file also contains the Clip information that was previously stored in the AACS1.DAT file. The following conditions apply to this file only.

BDCMF mising MasterID - SecureBDCMF requires VISAN or MasterID

This condition indicates that the `VISAN` *and* `MasterID` *elements are empty or do not exist in the BDCMF.CMF file. The VISAN or MasterID are used for identification of a 'BD-ROM Movie Media'. The BDCMF 1.10 specifications require either one or both.*

No PlayingTimeInfo Tag found in CMF!

The `PlayingTimeInfo` *element is required for a 'BD-ROM Movie Media'. This element describes the different codecs used in the Blu-ray Video and their duration. This message indicates it was not found in the BDCMF.CMF file.*

No CLipAV Files defined in the ClipAVFileInfo section

The `ClipAVFileInfo` *element contains information about the location and access method for ClipAV Files. This element and its child elements are required for Type A images only. If the image is Type B or later, this condition may be ignored.*

Parse Error

This is a generic parsing error message for the BDCMF.CMF file. There a few known errors that may cause the BDCMF.CMF file to fail loading. These causes are described by some of the messages in the Additional Info column. An unknown cause triggers this message.

AACS1.DAT

The AACS1.DAT file is present in BDCMF versions 0.90 or earlier. This file contains a `ClipAV` element which is used during encryption of an image. Therefore, the contents of this element are important only when the image is `Type A`. During the encryption process (`Type A` to `Type B` conversion), the Clip information is removed. However, if the Clip information is still present when the image is a `Type B` or later, it should be ignored.

AACS1.DAT: [*ErrorDescription*]. Line: [*LineNo*], Col: [*ColNo*]

An error occurred while parsing the AACS1.DAT file. This is typically caused by an XML formatting error in the file. If you are familiar with the structure of this file, you can open the file in a text editor and go to the line number and column numbers as given in this message to try to correct the problem. Otherwise, contact Eclipse Support for assistance.

Unknown Error - XML library reports no error!

This condition indicates that an unknown error occurred while parsing the AACS1.DAT file. This normally indicates a system error.

Common Conditions

The following conditions may occur on any XML file of a Blu-ray image.

[*filename*]: [*Description*]. Line: [*LineNo*], Col: [C*olNo*]

This is a generic parsing error message that may be triggered for any XML file. This is typically caused by an XML formatting error in the file. If you are familiear with the structure of the file specified by this message, you can open the file in a text editor and go to the line and column numbers as given by this message to try to correct the problem. Otherwise, contact Eclipse Support for assistance.

Parsing failure

This is a generic parsing error message for any XML file. There are some known errors that cause the file load to fail. Each of those is described above. Any unknown causes will trigger this message. Contact Eclipse Support for assistance.

Severity

This rule is considered an ERROR since it usually results in a failed analysis.

Cause

There can by several causes for this rule to be triggered. The most common cause is due to formatting errors in the files. This would indicate a problem in authoring or a problem with the tool that modified the part of the file that failed.

Solution

The solution depends on which of the above conditions triggered this rule. Contact Eclipse Support for further assistance.

Type:	Blu-ray
Reference:	BDCMF Specifications
Default Program Action:	Error

Rule ID: 890

BDCMF/PIC BCA Flag mismatch

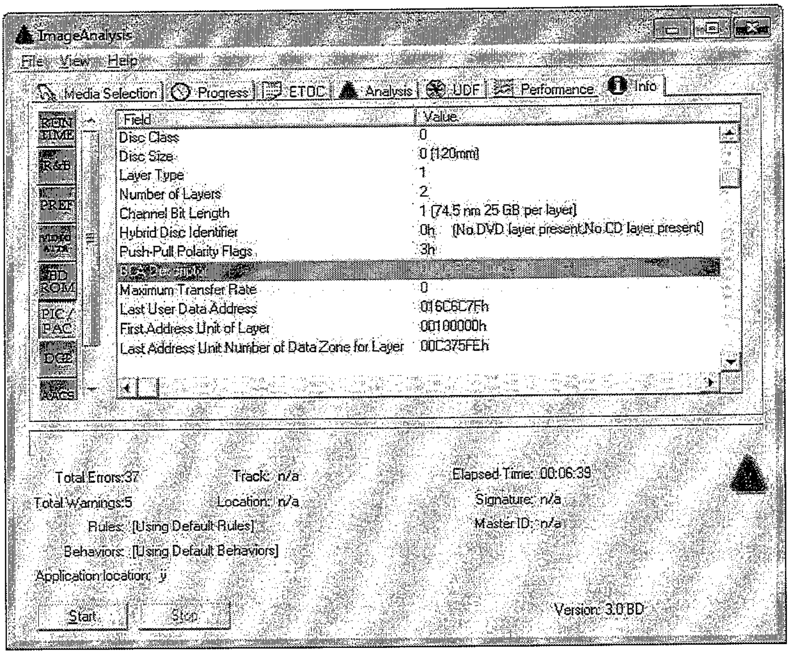
The BCA flag in the BDCMF.CMF and PIC.DAT files do not match.

Background

On a BDCMF image, the BCA flag indicates whether the final disc requires a BCA. On a disc, this would indicate whether the disc contains a BCA.

On an image, the BCA flag in the BDCMF.CMF file is used for informational purposes only. The BCA flag in the PIC.DAT file, on the other hand, will determine if the BCA flag is set on the final replica. The authoring system is responsible for making sure that this flag matches on both files.

To determine the setting for the BCA flag on the final disc, click Info | PIC/PAC. This will display the contents of the PIC data. The 'BCA Descriptor' will indicate whether the flag is set.



Field	Value
Disc Class	0
Disc Size	0 (120mm)
Layer Type	1
Number of Layers	2
Channel Bit Length	1 (74.5 nm 25 GB per layer)
Hybrid Disc Identifier	0h (No DVD layer present No CD layer present)
Push-Pull Polarity Flags	3h
[illegible]	
Maximum Transfer Rate	0
Last User Data Address	016C6C7Fh
First Address Unit of Layer	00100000h
Last Address Unit Number of Data Zone for Layer	00C375FEh

Total Errors:37
Track: n/a
Elapsed Time: 00:06:39
Total Warnings:5
Location: n/a
Signature: n/a
Rules: [Using Default Rules]
Master ID: n/a
Behaviors: [Using Default Behaviors]
Application location: ÿ
Version: 3.0 BD

Severity

This condition is considered an ERROR since it is unclear whether BCA is required.

Cause

This problem is typically caused by the authoring system when not setting both BCA flags the same.

Solution

The solution depends on whether or not BCA is required on the final disc and whether the BCA requirement matches the 'BCA Descriptor' setting in the PIC data.

If the customer's BCA requirement matches the BCA flag in the PIC data, then no further action is required and this error can be ignored. Otherwise, a new image may be required (or at least a new PIC.DAT file with the correct BCA setting).

Note that if you are using an Eclipse encoder for mastering, there is an option to override the BCA flag. Contact Eclipse Support for further assistance.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

Rule ID: 1827

BDCMF.SHA file processing error

An error occurred while trying to read the SHA-1 hash value from the BDCMF.SHA file.

Background

The BDCMF.SHA file is used to store a SHA-1 hash value for the BDCMF.CMF file. It was introduced in BDCMF Version 1.03 as optional but has become mandatory in BDCMF Version 1.10 and later.

The BDCMF.CMF file is always updated as a BD image moves through the pre-mastering and mastering process. If the BDCMF.SHA file is present, all utilities that update the BDCMF.CMF file must also update its SHA-1 hash value and store it in the BDCMF.SHA file. This error occurs when the EclipseSuite tools are unable to open the BDCMF.SHA file.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display more details with one of the following messages.

Error reading BDCMF.SHA file

This message indicates that the EclipseSuite tools failed to open the BDCMF.SHA file. This could be due to an access or other file system error in the computer being used.

This also indicates that the EclipseSuite tools will not be able to validate the SHA-1 hash for the BDCMF.CMF file.

Could not write new hash value

This message indicates that the EclipseSuite tools were unable to update the BDCMF.SHA file with a new SHA-1 hash value. The cause may be an access violation in the computer where the error occurred.

Since the EclipseSuite tools were unable to update the SHA-1 hash value, the next time the BD image is analyzed may result in a SHA-1 mismatch between the recalculated value and the one stored in the BDCMF.SHA file.

Severity

This rule is considered an ERROR since it indicates that the EclipseSuite tools were unable to read or update the BDCMF.SHA file. If the EclipseSuite tools were unable to read the file, then it also means that they will not be able to validate the SHA-1 hash. If the EclipseSuite tools were unable to write the new SHA-1 hash value, it also means that the next time the image is analyzed it may result in a SHA-1 mismatch between the recalculated SHA-1 hash and the one stored in the BDCMF.SHA file.

Cause

This rule was created to catch conditions where the EclipseSuite tools are unable to read/write the BDCMF.SHA file. At this point, there are no known conditions that would trigger this rule. However, the Windows operating system includes several security attributes that can trigger this rule. For example, if the file's Read-Only attribute is set, then the EclipseSuite tools cannot update it.

Solution

While this error can be triggered by several conditions, it is more likely to be caused by file attributes or Windows file security attributes. Verify that the file is accessible and that the user who is currently logged in has read/write privileges to the image directory.

NOTE
This error is specific to the integrity of the BDCMF.CMF file and not the user data. As of this writing, BDCMF 1.03 and 1.10 were not common and it is possible that some utilities may not know how to update the BDCMF.SHA file. This may result in a good analysis of the image but bad SHA-1 for the BDCMF.CMF file.

Type:	Blu-ray
Reference:	BDCMF Specifications Version 1.03 and later
Default Program Action:	Error

Rule ID: 1615

BDCMF.SHA value does not match BDCMF.CMF file

The calculated SHA-1 hash value for the BDCMF.CMF file does not match the SHA-1 hash value stored in the file BDCMF.SHA.

Background

The BDCMF.SHA file is used to store a SHA-1 hash value for the BDCMF.CMF file. It was introduced in BDCMF Version 1.03 as optional but has become mandatory in BDCMF Version 1.10 and later.

The BDCMF.CMF file is always updated as a BD image moves through the pre-mastering and mastering process. If the BDCMF.SHA file is present, all utilities that update the BDCMF.CMF file must also update its SHA-1 hash value and store it in the BDCMF.SHA file. This error occurs when the calculated SHA-1 value does not by the value stored in the BDCMF.SHA file.

NOTE
This error is specific to the integrity of the BDCMF.CMF file and not the user data. As of this writing, BDCMF 1.03 and 1.10 were not common and it is possible that some utilities may not know how to update the BDCMF.SHA file. This may result in a good analysis of the image but bad SHA-1 for the BDCMF.CMF file.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display the expected SHA-1 has value.

Severity

This rule defaults to an ERROR since it is unknown if the BDCMF.CMF file is corrupt or if the utility that last updated the BDCMF.CMF file did not update the SHA-1 has value.

Cause

This error normally occurs when the utility that last updated the BDCMF.CMF file did not update the SHA-1 hash in the BDCMF.SHA file. Since the use of the BDCMF.SHA file is relatively new in BDCMF 1.03 specifications, this will normally happen with utilities that do not fully support this revision of the BDCMF specifications. It is also possible, but less likely, that the BDCMF.CMF file is corrupt.

Solution

It is more likely that the last utility that updated the BDCMF.CMF file did not update the SHA-1 hash value. Therefore, make sure that the utilities you are using for processing the BD image fully support BDCMF 1.03 and later versions. Since it is also possible that a corrupt BDCMF.CMF file may trigger this rule, normally it would be expected that other errors would also occur. If this is the only error then it likely not a problem. However, contact Eclipse Customer Support in order to validate the severity of this condition.

Type:	Blu-ray
Reference:	BDCMF Specifications Version 1.03 and later
Default Program Action:	Error

Rule ID: 1614

BD-J application profile

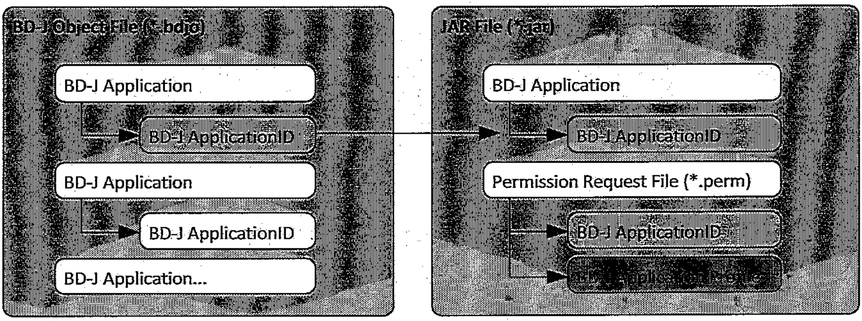
This is an informational message that identifies the profile in which a BD-J Application can execute.

Background

Each BD-Java application includes a permission request file that specifies the BD-Player profile in which the application can execute. For example, BD-Java applications which take advantage of BD-Live features require a Profile 2 BD player.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will identify the profile.


BD-J Object File (*.bdjo)
BD-J Application
BD-J ApplicationID
BD-J Application
BD-J ApplicationID
BD-J Application...
JAR File (*.jar)
BD-J Application
BD-J ApplicationID
Permission Request File (*.perm)
BD-J ApplicationID

[*BDJOFile*] [*AppID*], [*JARFile*], [*PermissionRequestFile*] [*MovieStudio*], '[*Profile*]'

This message identifies the player profile required to run the specified BD-J application.

[*BDJOFile*] [*AppID*], [*JARFile*], [*PermissionRequestFile*] **MovieStudio:** [*MovieStudio*], **Producer:** [*Producer*] '[*Profile*]'

This message identifies the player profile required to run the specified BD-J application.

Severity

This rule is for information purposes only. Therefore, it is considered an INFO severity level.

Cause

N/A.

Solution

N/A.

Type: Blu-ray
Reference: Blu-ray Specifications, Section 3-2: BD-Java Specifications
Default Program Action: Info

Rule ID: 1649

BD-J application signer

This is an informational message that identifies the signer of a certificate.

Background

The entity (e.g. organization) that signs a BD-Java application is identified via the **Issuer and Serial Number** field in the **SignerInfo** structure in the Signature Block File. This field matches the **Subject** and **Serial Number** fields of a **tbsCertificate**.

Signature Block File Syntax	
Content Info	
Content Type	Identifies the content structure of the Signature Block File. In Blu-ray, this specifies "Signed Data".
Content	This field is a structure that describes the contents of the Signature Block File. The structure depends on the Content Type field. When the Content Type specifies "Signed Data", this field has the syntax as described in the following table.

Content Syntax	
Version	= "1"
Digest Algorithm Identifier	= "SHA-1"
Content Info	This field is a structure similar to the one above. However, when it is inside a **Content** structure, the Content Type must be set to "Data" and the Content is the Signature File contents.
	Content Type = "Data"
	Content Signature File contents.
Certificates	One or more certificate chains.
Signer Info	A structure that identifies the signer and an encrypted digest for the Signature File. This structure has the syntax as described in the following table.

Signer Info Syntax	
Version	= "1"
Issuer and Serial Number	Identifies the signer's certificate via the Issuer Distinguished Name and Issuer-specific Serial Number, both of which are also found in a certificate in the Certificates field of the Content.
Digest Algorithm	= "SHA-1". The algorithm used to generate a digest for the Signature File.

Digest Encryption Algorithm	= "RSA", the algorithm used to encrypt the digest for the Signature File.
Encrypted Digest	The encrypted digest for the Signature File.

Additional Info

When this rule is triggered, the **Additional Info** column will display a message identifying the entity (e.g. organization) which signed the BD-Java application.

Severity

This rule is for information purposes only. Therefore, it is considered an INFO severity level.

Cause

N/A.

Solution

N/A.

Type: Blu-ray
Reference: Blu-ray Specifications, Section 3-2: BD-Java Specifications
Default Program Action: Info

Rule ID: 1645

BD-J Object file error

A BD-J Object file contains an invalid file type indicator or a bad file version number.

Background

All BD-J Object files (*.bdjo) start with a header where the first four bytes are set to "BDJO", identifying the file as a BD-J Object. The header also includes a version field to specify the version of file as "0100" or "0200".

BD-J Object File Syntax (xxxxx.bdjo)	
Field	**Description**
Type Indicator	="BDJO"
Version Number	= "0200" or "0100" (it is recommended to use a value of "0200")
TerminalInfo	Start address of *TerminalInfo()**.
AppCacheInfo	Start address of *AppCacheInfo()**.
TableOfAccessiblePlayLists	Start address of *TableOfAccessiblePlayLists()**.
ApplicationManagementTable	Start address of *ApplicationManagementTable()**.
KeyInterestTable	Start address of *KeyInterestTable()**.
FileAccessInfo	Start address of *FileAccessInfo()**.
TerminalInfo	

AppCacheInfo
TableOfAccessiblePlayLists
ApplicationManagementTable
KeyInterestTable
FileAccessInfo

** Relative to the start of the xxxxx.bdjo file.*

This error indicates that a different file type or file version was specified.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will indicate which condition triggered this rule.

Invalid type_indicator field

This message indicates that the BD-J Object file has an invalid file type indicator. All BD-J Object files start with a header where the first four bytes identify the file as a BD-J Object file ("BDJO").

Invalid version_number field

This message indicates that the file version field contains an invalid value. All BD-J Object files start with a header where the first four bytes identify the file as a BD-J Object file ("BDJO") and the next four bytes identify the file's version number ("0100" or "0200").

Severity

This condition is considered an error since it would indicate that the file is corrupt or that the wrong address to the file has been specified.

Cause

It is unknown what causes this condition. However, it is possible that it occurred when the image was authored.

Solution

Contact Eclipse Customer Support for assistance.

Type:	Blu-ray
Reference:	Blu-ray Disc Read-Only Format 2.0 Part 3: Audio Visual Basic Specifications (3-2 BD-J Specifications)
Default Program Action:	Error

Rule ID: 1604

BD-J object file not on disc

A BD-Java file was not found on the disc.

Background

When analyzing a Blu-ray disc, the EclipseSuite tools parse through the navigation structure to determine the mapping between the Index Table, CPS Units, Titles, PlayLists, PlayItems and Clips. These objects typically refer to actual files on the media. As references to these files are found, each file is loaded and analyzed. This rule is triggered when parsing through BD-J object files and a file is missing from the expected location.

Severity

This rule indicates that a file is missing. Therefore, it is considered a serious ERROR.

> **NOTE**
> *This error may be referring to a file that will eventually be downloaded from an online server by the end-user. Currently, the EclipseSuite tools cannot determine if the object is to be downloaded or whether it is intended to be on the disc. This rule is, therefore, set to WARNING. In the event this rule is triggered, consult the author to determine if the missing file should have been included in the image.*

Cause

This condition is caused by the authoring system that created the image.

Solution

Contact Eclipse Support for further assistance.

Type:	Blu-ray
Reference:	Blu-ray Disc Read-Only Format Part 3: Audio Visual Specifications (3-2 BD-J Specifications)
Default Program Action:	Warning

Rule ID: 1568

BD-J Signed Application

This is an informational message that identifies a Blu-ray image that includes BD-J applications.

Type:	Blu-ray
Reference:	Blu-ray Disc Read-Only Format Part 3: Audio Visual Basic Specifications
Default Program Action:	Info

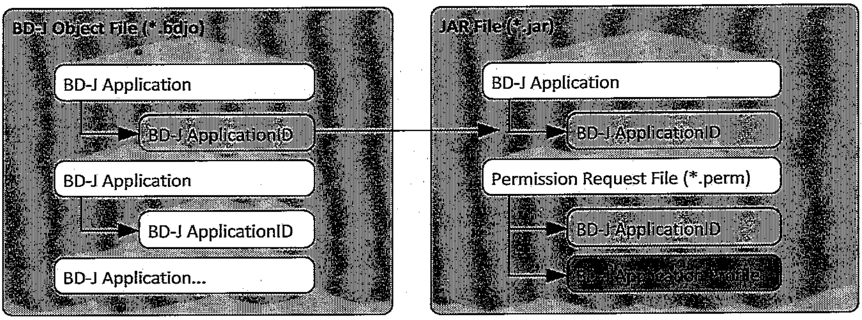
Rule ID: 1618

BD-J Xlet Application ID mismatch

The Application ID in the BD-J Permission Request File does not match the Application ID defined in the BD-J Object file.

Background

The BD-J Permission Request file determines access permissions to a signed BD-J application. A BD-Object contains information related to a BD-J Title. Each BD-J Object information is stored a file with the filename format "xxxxx.bdjo", where xxxxx is any digit, and it is stored in the \BDMV\BDJO directory. Each BD-J Object file includes a list of BD-J Applications where each BD-J Application contains a unique ID. Each BD-J Application is associated with a Permission Request File, which also contains the Application ID. This error indicates that the Application ID defined in the BD-J Object file and in the BD-J Permission Request file do not match.


BD-J Object File (*.bdjo)
BD-J Application
BD-J ApplicationID
BD-J Application
BD-J ApplicationID
BD-J Application...
JAR File (*.jar)
BD-J Application
BD-J ApplicationID
Permission Request File (*.perm)
BD-J ApplicationID
BD-J Application Profile

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will identify the actual and expected values.

[*PermReqAppID*]. '[*BDObjectFile*]' [*AppID*], '[*JARFile*]', '[*PermReqFile*]'

This message identifies the following items:

- *PermReqAppID: The Application ID that was found inside the Permission Request File.*
- *BDObjectFile: The BD-J Object file (xxxxx.bdjo) where the BD-J Application is described.*
- *AppID: The Application ID that is assigned to the BD-J Application in the BD-J Object file.*
- *JARFile: The JAR File that contains the Permission Request File for the BD-J Application.*
- *PermReqFile: The Permission Request File for the BD-J Application.*

Severity

It is unknown whether this condition will have any effect in playability. Although the default severity is an ERROR, since each permission request file includes properties of the BD-J application you should check with the author to determine the severity.

Cause

This condition is typically caused by the authoring system that created the image.

Solution

Check with the author to determine if this is intended or whether the image will have to be re-authored.

Type:	Blu-ray
Reference:	Blu-ray Specifications, Section 3-2: BD-Java Specifications

Default Program Action: Error

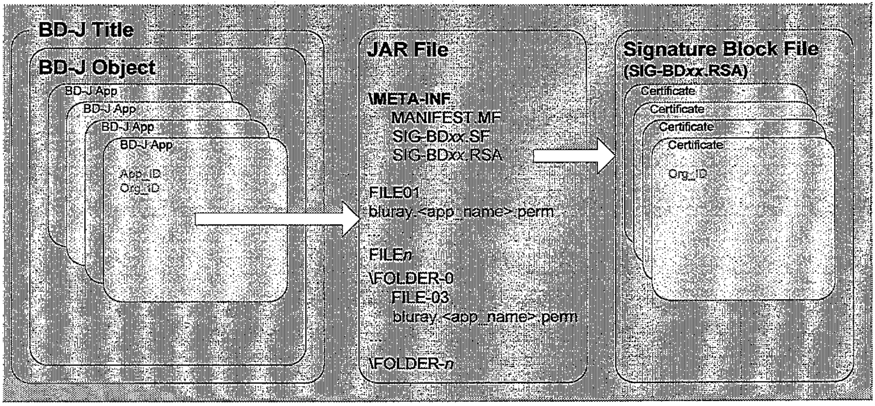
Rule ID: 1606

BD-J Xlet Organization ID mismatch

The Organization ID for a BD-J Application does not match the Organization ID in the application's Permission Request File and Signature Block File.

Background

Each BD-J Title contains a single BD-J Object file (*.bdjo), which identifies the BD-J Applications associated with the title. Each BD-J Application includes an Application ID and Organization ID and contains references to a JAR File where the application files are stored. A BD-J Application may contain a Permission Request File in the same folder as the initial file of the BD-J application inside the JAR File. The Permission Request File must also include a matching Organization ID. The JAR File also includes a Signature Block File. The Signature Block File contains certificates for authentication. Each Certificate also includes a matching Organization ID. This error indicates that a BD-J Application, Permission Request File and Certificate did not all have a matching Organization ID.


BD-J Title
BD-J Object
BD-J App
BD-J App
BD-J App
BD-J App
App_ID
Org_ID
JAR File
\META-INF
MANIFEST.MF
SIG-BDxx.SF
SIG-BDxx.RSA
FILE01
bluray.<app_name>.perm
...
FILEn
\FOLDER-0
FILE-03
bluray.<app_name>.perm
...
\FOLDER-n
Signature Block File
(SIG-BDxx.RSA)
Certificate
Certificate
Certificate
Certificate
Org_ID

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will identify the actual and expected values.

'[*JARFile*]', '[*SignatureBlockFile*]': cert([*CertSN*] | [*CertIndex*]), Expected '[*Expected_OrgID*]' instead of '[*Actual_OrgID*]'

This message is displayed when the Organization ID in a certificate does not match the Organization ID in a BD-J Application.

This message displays the expected and actual values and also the JAR File that contains the Signature Block File where the certificate is stored. It also displays the Certificate Serial Number and its index within the Signature Block File.

Expected '[*Expected_OrgID*]' instead of '[*Actual_OrgID*]'. '[*BDJObjectFile*]' [*AppID*], '[*JARFile*]', '[*PermissionRequestFile*]'

This message is displayed when the Organization ID in a BD-J Application Permission Request File does not match the Organization ID in the BD-J Application.

This message displays the expected and actual values and also the JAR File that contains the Permission Request File. It also identifies the BD-J Object file where the Application is identified.

Severity

It is unknown whether this condition will have any effect in playability. Therefore, it is considered an ERROR.

Cause

This condition is typically caused by the authoring system that created the image.

Solution

The image will have to be re-authored.

Type:	Blu-ray
Reference:	Blu-ray Specifications, Section 3-2: BD-Java Specifications
Default Program Action:	Error

Rule ID: 1605

BD-Java

This rule identifies the BD-Java content of a BD disc or image.

Background

BD-J is one of two possible logical structures of a BD-ROM. A typical Blu-ray video uses the BDMV structure, or Movie Object. BD-J, on the other hand, provides a fully programmable application environment with network connectivity, thereby enabling authors to create highly interactive, updateable BD-ROM titles.

Type:	Blu-ray
Reference:	Blu-ray Disc Read-Only Format Part 3: Audio Visual Specifications (3-2 BD-J Specifications)
Default Program Action:	Info

Rule ID: 1524

BD-Live

This is an informational message that identifies BD-Live content on a Blu-ray image.

Type:	Blu-ray
Reference:	BDCMF Specifications

Default Program Action: Info

Rule ID: 1525

BDMV ID

This is an informational message that displays the Identification Data from the bd.bdmv file.

Background

The bd.bdmv file is present when a Blu-ray Video includes BD-Java content. It is used for identification purposes. The ID consists of an Organization ID, which identifies the owner of the content on the disc, and a Disc ID, which uniquely identifies the disc. The **Additional Info** column in the Analysis will display the ID. The file is stored in the \CERTIFICATE folder.

BDMV ID File

Field Name	Description	
type_indicator	="BDID", identifies the bd.bdmv file.	
version_number	="0200" or "0100", identifies the bd.bdmv file version	
reserved	= 00h	
ID_Data()	Organization_ID	Identifies the organization ID of the disc, which is used to construct a Virtual Package binding unit for the disc.
	Disc_ID	Iidentifies the disc ID of the disc, which is used to construct a Virtual Package binding unit for the disc.
	Reserved	= 00h

Type: Blu-ray

Reference: Blu-ray Disc Read-Only Format
Part 3: Audio Visual Basic Specifications, Section 5.10

Default Program Action: Info

Rule ID: 1601

BDMV ID file error

The bd.bdmv file contains invalid field data.

Background

The bd.bdmv file is present when a Blu-ray Video includes BD-Java content. It is used for identification purposes. The ID consists of an Organization ID, which identifies the owner of the content on the disc, and a Disc ID, which uniquely identifies the disc. During analysis, the contents of this file are validated. This error is triggered if the contents are invalid.

BDMV ID File

Field Name	Description	
type_indicator	="BDID", identifies the bd.bdmv file.	
version_number	="0200" or "0100", identifies the bd.bdmv file version	
reserved	= 00h	
ID_Data()	Organization_ID	Identifies the organization ID of the disc, which is used to construct a Virtual Package binding unit for the disc.
	Disc_ID	Iidentifies the disc ID of the disc, which is used to construct a Virtual Package binding unit for the disc.
	Reserved	= 00h

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will identify the field containing the invalid data with one of the following messages.

type_indicator field is not 'BDID'

This message is displayed when the type_indicator field IS NOT set to "BDID", which identifies the bd.bdmv file.

Version_number field is not '0200' nor '0100'

This message is displayed when the version_number field IS NOT set to one of the two valid versions.

Reserved field is not all zeros

This message is displayed when the EclipseSuite tools find that the reserved fields contain non-zero data.

Severity

It is unknown if invalid data in any of these fields will affect playability. However, since the specifications have defined the value for each of the fields, this condition is considered an ERROR if any of them are not set accordingly.

Cause

This condition is typically caused by the authoring system that created the file.

Solution

The image needs to be re-authored.

Type:	Blu-ray
Reference:	Blu-ray Disc Read-Only Format Part 3: Audio Visual Basic Specifications, Section 5.10
Default Program Action:	Error

Rule ID: 1602

BD-R File System

This rule is triggered when the Eclipse software identifies the BD-R File System. The file system on a BD-R is similar to that of a BD-ROM. However, the file system on a BD-R includes recording features that are not supported on a BD-ROM.

Type:	Exclusion
Reference:	N/A
Default Program Action:	Info

Rule ID: 825

BD-RE File System

This rule is triggered when the Eclipse software identifies the BD-RE File System. The file system on a BD-RE is similar to that of a BD-ROM. However, the file system on a BD-RE includes recording features that are not supported on a BD-ROM.

Type:	Exclude
Reference:	N/A
Default Program Action:	Info

Rule ID: 826

BD-ROM AACS robustness requirement failure

The Blu-ray Video content of the image is not protected with AACS.

Background

This rule is used to identify Blu-ray Video images that are not encrypted with AACS. The Blu-ray specifications require that all Blu-ray video images be protected with AACS. If not, then any playback device must abort playback. This rule can also be triggered on a DVD image that includes Blu-ray Video content.

Severity

This is considered an ABORT condition since there is a high probability that it will cause playback problems.

Cause

This problem is caused by the authoring system when no AACS encryption was applied to the image.

Solution

The image must be re-authored.

Type:	Blu-ray
Reference:	Blu-ray Specifications
Default Program Action:	Abort

Rule ID: 1640

BD-ROM Content Category

This is an informational rule that identifies whether a BDCMF Blu-ray image is one of the following:

- BD-ROM MOVIE MEDIA
- BD-ROM MOVIE MEDIA WITH BD DATA
- BD-ROM DATA MEDIA

Type:	Blu-ray
Reference:	BDCMF Specifications
Default Program Action:	Info

Rule ID: 1794

BD-ROM directory and file names should not contain space characters

The Blu-ray Video specifications strongly discourage the use of space characters (0x20) in directory and file names.

Background

In order to maintain compatibility, the Blu-ray Video General Authoring Recommendations strongly recommend the use of filenames which **do not contain** spaces.

Additional Info

When this rule is triggered, the **Additional Info** column in the analysis will identify the filename in question.

'[*BDJObjectFile*]' [*BD-JAppID*], '[*JARFilename*]', '[*Filename*]'

This message indicates that the EclipseSuite tools found a file inside a JAR file whose filename includes space characters. The filename is identified with this message.

"[*FileName*]"

This message identifies the filename whose name includes space characters.

Severity

Although there are no reports of playability problems, this condition is considered an ERROR.

Cause

This condition is caused during authoring of the image.

Solution

The image must be re-authored.

Type:	UDF
Reference:	Blu-ray Disc Read-Only Format Part 34: Audio Visual Specifications (Guidelines)

	Chapter 14: General Authoring Recommendations
Default Program Action:	Error

Rule ID: 1714

BD-ROM File System

This is an informational message that identifies the BD-ROM File System on an image.

Type:	Exclusion
Reference:	BD-ROM File System Specifications
Default Program Action:	Info

Rule ID: 794

BD-ROM Producer

This is an informational message that identifies the producer of the Blu-ray Video image.

Background

This rule is part of the Title Structure analysis of EclipseSuite. The Title Structure analysis includes a list of movie studios that are supported. For each movie studio, there is a list of 'authorized' producers (e.g. authoring studios). When the Title Structure analysis is being performed on an image, the producer is identified in the image and this rule is triggered to identify it in the EclipseSuite analysis.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Info

Rule ID: 1620

BDROM/BDR Hybrid Format Error

The BDCMF.CMF file identifies the image as a BD-ROM/BD-R Hybrid but the user control data does not.

Background

The BDCMF.CMF file includes a field that indicates whether an image is Hybrid image (BD with CD or DVD). On a BD9, the CPS Sector of the user Control data includes a flag that also specifies whether the image is hybrid.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display more details.

UCD flags=x[*Actual*], expected 0x03

This message shows the actual and expected values. The flag value 03h identifies a hybrid image (BD9).

Type:	Blu-ray

Reference:	BDCMF & Blu-ray Read-only Specifications
Default Program Action:	Error

Rule ID: 1679

Binding Unit Root Certificate

The explanation for this title check rule contains confidential information. Please refer to the studio-specific supplemental rules help PDF document. The document is available from Eclipse Support.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Info

Rule ID: 1666

Blu-ray AACS File on layer 1

An AACS file was found on layer 1.

Background

The AACS specifications require that all AACS related files be recorded on layer 0. This rule is triggered if any of the following files are recorded in layer 1.

\AACS\CONTENT000.CER
\AACS\DUPLICATE\CONTENT000.CER
\AACS\CONTENTHASH000.TBL
\AACS\DUPLICATE\CONTENTHASH000.TBL
\AACS\CONTENTREVOCATION.LST
\AACS\DUPLICATE\CONTENTREVOCATION.LST
\AACS\MKB_RO.INF
\AACS\DUPLICATE\MKB_RO.INF
\AACS\MKB_RW.INF
\AACS\DUPLICATE\MKB_RW.INF

Severity

This condition does not indicate a non-conformance to the AACS specifications. However, it does not indicate that there will be playability problems. Therefore, this condition is considered a FLAG severity.

Cause

This condition is caused during authoring of the image.

Solution

To fix this condition, the image must be re-authored.

Type:	Blu-ray
Reference:	N/A

Default Program Action: Flag

Rule ID: 1747

Blu-ray CMF Format Error

The EclipseSuite programs detected missing or invalid data in the BDCMF.CMF file.

The BDCMF.CMF file is the primary file that describes a BD image. It contains references to other files that make up the image and provides details of those files. The BDCMF.CMF file is formatted in XML. When this rule is triggered, it indicates that an XML element, attribute or value is invalid or missing.

Additional Info

When triggered, the **Additional Info** column in the analysis will display the specific cause of this error with one of the following messages.

Layer 0 number of sectors ([*TotalSectors*]) must be divisible by 32 sectors (a cluster size)

The BDCMF.CMF file specifies a layer 0 size which is not divisible by 32. The layer 0 size should be represented in sectors and must be evenly divisible by the cluster size, which is 32 sectors.

Image Data (UD.DAT) reference missing

The reference to the user data file UD.DAT is missing in the BDCMF.CMF file. This reference is required since it describes the file that contains the user data, its size, etc. Without this reference, it would not be possible to process this image.

Example:

```
<File Type="UserData" Name="UD.DAT" Size="8630894592">
    <StartPSN>00100000</StartPSN>
    <HashValue Type="SHA-1">2341234123412341234123412341234123412341</HashValue>
</File>
```

Reference: BDCMF Specifications version 0.90 pg. x

Image Data (UD.DAT) Start PSN expected (100000) actual ([*ActualPSN*])

The BDCMF.CMF file includes the wrong start address for the user data (UD.DAT). All Blu-ray images start at PSN 0x100000.

User Control Data (UCD.DAT) Start PSN expected (100000) actual ([*ActualPSN*])

The BDCMF.CMF file includes the wrong start address for the user control data (UDC.DAT). The user control data in all Blu-ray images should be recorded starting at PSN 0x100000.

Disc Capacity Unknown

The BDCMF.CMF file is missing the 'Density' XML attribute, it contains an invalid value or a density value has not been specified. The 'Density' attribute specifies the disc capacity as: 23GB, 25GB, 27GB 46GB, 50GB or 54GB.

PIC Data (PIC.DAT) reference missing

The reference to the PIC.DAT file is missing in the BDCMF.CMF file. The PIC.DAT file is required since it specifies control data information and other vital information required for processing and playback.

Example:

```
<File Type="PICData" Name="PIC.DAT" Size="65536">
    <HashValue Type="SHA-1">1234123412341234123412341234123412341234</HashValue>
</File>
```

Control Data (CONTROL.DAT) reference missing

The BDCMF.CMF file is missing a reference to the CONTROL.DAT file.

PAC Data for Layer 0 (PAC.DAT) reference missing

The reference to the PACL0.DAT file is missing in the BDCMF.CMF file. The PACL0.DAT file is required since it specifies information that will be recorded on to the media during mastering.

Example:

```
<File Type="PACDataLayer0" Name="PACL0.DAT" Size="65536">
    <HashValue Type="SHA-1">4123412341234123412341234123412341234123</HashValue>
</File>
```

PAC Data for Layer 1 (PAC.DAT) reference missing

The reference to the PACL1.DAT file is missing in the BDCMF.CMF file. The PACL1.DAT file is required since it specifies information that will be recorded on to the media during mastering.

Example:

```
<File Type="PACDataLayer1" Name="PACL1.DAT" Size="65536">
    <HashValue Type="SHA-1">4123412341234123412341234123412341234123</HashValue>
</File>
```

Cause

This problem is typically caused by the authoring application that created the BD image.

Severity

This rule is considered an error since it may be impossible for a pre-mastering or mastering system to process this image.

Solution

It is possible that some of these conditions may be corrected by manually editing the BDCMF.CMF file. However, you must be familiar with the CMF specifications and know what changes need to be made. If editing is not possible, then the image must be re-authored.

Type:	Blu-ray
Reference:	BDCMF Specifications
Default Program Action:	Error

Rule ID: *844*

Blu-ray Content Certificate ID Data

This is an informational message that identifies the Applicant ID and Content Sequence Number from the Content Certificate of the image.

Type:	Blu-ray

Reference: N/A
Default Program Action: Info

Rule ID: 1835

Blu-ray Last User Data Address too large

The layer size is greater than the maximum allowed by the specifications.

Background

On a BDCMF image, the layer 0 size is specified in the BDCMF.CMF and PIC.DAT files. On a dual-layer image, the layer 1 size is calculated using the layer 0 size and the UD.DAT size. The maximum number of sectors on layer 0 and 1 are pre-defined by the specifications based on the Channel bit length and other physical parameters.

On a replica, the PIC data specifies the start address and maximum end address for layer 0 and layer 1. This rule is triggered if the values specified by the BDCMF.CMF or PIC.DAT files exceed the maximum allowed by the specifications.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display details indicating the cause of this error with one of the following messages.

Layer 0 Sectors [*Actual*], Maximum allowed [*MaxAllowed*]

This message is displayed when the layer 0 size, as specified in the BDCMF.CMF file, is greater than the maximum allowed by the specifications.

The Actual value refers to the number of sectors specified in the BDCMF.CMF file. The MaxAllowed is either CA73FEh or D950BEh depending on whether the Channel bit length is 74.5 nm or 69.0 nm.

PIC LUDA [*Actual*], Maximum allowed [*MaxAllowed*]

This message is displayed when the last sector of user data specified in the PIC.DAT file exceeds the maximum allowed by the specifications.

The Actual value refers to the number of sectors specified in the PIC.DAT file. The MaxAllowed is either CA73FEh or D950BEh depending on whether the Channel bit length is 74.5 nm or 69.0 nm.

Layer 1 Last User Data Address [*Actual*], Maximum allowed [*MaxAllowed*]

This message is displayed when the last user data address on layer 1, as specified in the PIC.DAT file, exceeds the maximum allowed by the specifications.

The Actual value is the value specified in the PIC.DAT. The MaxAllowed is the maximum value allowed by the specifications.

Severity

This condition is considered an error since the image (layer) length exceeds the maximum allowed.

Cause

This problem is normally caused by the authoring system that created the image.

Solution

The image may have to be re-authored. Please contact Eclipse Support.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

Rule ID: 1680

Blu-ray Layer 1 length greater than layer 0

There is more data stored on layer 1 than there is on layer 0.

Background

Dual-layer Blu-ray images are recorded in opposite track path (OTP) only. In this method, the user data sector addresses on layer 1 are the same ones used on layer 0, except they are bit-inverted. This means that the amount of user data on layer 1 cannot exceed the same amount that is recorded on layer 0 (i.e. layer 1 length must be <= length of layer 0).

This problem has been seeing on some recordable media. While this may not affect playability on recordable media, it is not valid on a replicated disc. Therefore, if a recordable media is delivered and it is to be used as a master for replication, this condition would be considered an error.

Severity

This condition is considered an error since it is not possible to master such an image.

Cause

This problem has been seen on recordable media. Although it may not present a problem on recordable media, the authoring software that recorded the media should not have recorded more data on layer 1.

Solution

So far this condition has only been seen on recordable media that is used for mastering purposes. If copied to hard disk as a BDCMF image, it may result in an invalid image. The media should be re-authored/re-recorded, with a different authoring application that does not have this problem.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

Rule ID: 1746

Blu-ray Recordable (BD-R)

This is an informational message that identifies Blu-ray Recordable media.

Type:	Exclude
Reference:	N/A
Default Program Action:	Flag

Rule ID: 869

Blu-ray Rewritable (BD-RE)

This is an informational message that identifies Blu-ray Rewritable media.

Type:	Exclude
Reference:	N/A
Default Program Action:	Flag

Rule ID: 870

Blu-ray ROM

The image being analyzed is identified as a Blu-ray ROM.

Additional Info

When this rule is triggered, the Additional Info column in the Analysis may display additional message that will further describe the format.

- BD-ROM MOVIE MEDIA
- BD-ROM MOVIE MEDIA WITH BD DATA
- BD-ROM DATA MEDIA

Type:	Exclusion
Reference:	Blu-ray Specifications
Default Program Action:	Info

Rule ID: 678

Blu-ray Unit Usage File Error

The EPN and CCI fields in a CPS Unit Usage file do not match.

Background

The EPN bit flag indicates the value of the Encryption Plus Non-assertion. The EPN bit should be set when the CCI field is set to 00b (Copy Control Not Asserted = Unencrypted CPS Unit). This rule indicates that both CCI and EPN fields are set to 0.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display more details.

CPS Unit ([*CPSUnitNo*]) EPN([*EPNValue*]) CCI([*CCIValue*])

This message identifies the CPS Unit Usage file and the EPN and CCI values. For an unencrypted CPS Unit, the CCI value should be 00b and the EPN should be set to 1.

Severity

It is unknown as to how this will affect playability. Therefore, this is considered an ERROR.

Cause

This problem is caused by the authoring system that created the image.

Solution

The image must be re-authored. Contact Eclipse Customer Support for further assistance.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

Rule ID: 1648

Both 3D Clips contain M2TS Specific Areas

The 3D specifications require that only one of the two M2TS files can have an 'M2TS Specific Area'.

Background

The 3D specifications include an M2TS file for the left eye and one for the right eye. The M2TS file for the left eye is used for 2D playback and both left and right eye M2TS files are used for 3D playback. The 3D specifications include an SSIF file which is a combination of the left and right eye. However, there are some areas of the M2TS files that it may not include. These areas are called 'M2TS Specific Areas'. These areas can only exist on one of the two M2TS files but not on both. This rule indicates that both M2TS files include 'M2TS Specific Areas'.

Additional Info

When this condition occurs, the **Additional Info** column in the Analysis will display more details.

Detected between '[*SSIF_File*]', '[*M2TS_File*]' and '[*M2TS_File*]'

This message identifies the SSIF and M2TS files affected by this condition.

Severity

It is unknown how this will affect playability. Therefore, this condition is treated as an ERROR.

Cause

This condition is caused by the authoring system that created the image.

Solution

The image must be re-authored. However, as of this writing, the 3D specifications were not yet finalized. Check with the author of the image to verify the severity of this condition.

Type: 3D-BD
Reference: 3D Specifications
Default Program Action: Error

Rule ID: 1730

Bus encrypted sector not in Clip AV stream file space

A sector that does not belong to a Clip AV Stream file has been tagged for Bus Encryption.

Background

Bus encryption is another layer of data protection. Flags can be set to indicate whether the data transferred between a drive and host PC will be encrypted. The User Control Data (UCD) includes the Bus Encryption Enabled flag for every sector of an image. However, the flag should only be set for sectors belonging to files in the \HDMV\STREAM directory. This error indicates that the BEF flag is set for a sector that does not belong to a Clip AV Stream file.

The User Control Data file includes properties that describe each sector of user data. One property is the Bus Encryption Enable flag (BEE). Similarly, the Content Certificate file(s) include the Bus Encryption Flag (BEF) for the ClipAV sectors described by the content certificate file. In case of a dual-layer image, both Content Certificate files must reflect the same Bus Encryption status. The EclipseSuite tools make sure that the Bus Encryption status specified in the User Data and Content Certificate file(s) is consistent.

All Clip AV files (*.m2ts) are made up of Aligned Units consisting of 3 logical sectors. The CPI bits are at the beginning of an Aligned Unit and indicate whether the Aligned Unit is encrypted. When the Bus Encryption flag is set for any of the sectors in the Aligned Unit, then the CPI bits must also be set.

> **NOTE**
> *The use of Bus Encryption flag has been supported since BDCMF 1.10. However, hardware support has not been implemented yet. The Blu-ray specifications require that new drives manufactured starting July 1, 2011 must support Bus Encryption.*

Additional Info

When this error occurs, the **Additional Info** column of the Analysis will display more details.

UCD: [***Enabled/Disabled***], Sector: [***Encrypted/Unencrypted***], CC: [***Enabled/Disabled***]
This message identifies one of the following conditions:

- *BEE = 1, BEF = 0, CPI = 01, 10 or 11*

  The bus encryption status specified by the BEF flag in the User Control Data (UCD.DAT) does not match the BEE flag in the Content Certificate file and CPI bits of the sectors.

- *BEE = 0, BEF = 1, CPI = 01, 10 or 11*

  The bus encryption status specified by the BEE flag in the Content Certificate file does not match the BEF and CPI bits.

- *BEE = 1, BEF = 1, CPI = 00*

  The CPI bits in an Aligned Unit do not match the BEF flag in the UCD. The UCD includes a BEF flag for each sector.

Severity

This condition is considered an error since it is not allowed to set the BEF on sectors that are not in the \HDMV\STREAM folder. This condition may also result in playability problems.

Cause

This condition is normally caused by the authoring system.

Solution

The image must be re-authored. Contact Eclipse Customer Support for further assistance.

Type:	Blu-ray
Reference:	Blu-ray AACS Specifications
Default Program Action:	Error

Rule ID: 1855

Bus Encryption disabled

This is an informational rule that specifies that the Bus Encryption Enabled (BEE) flag IS NOT SET in the Content Certificate file(s).

Background

The Bus Encryption Enabled flag indicates whether a player should transfer encrypted data to an application. This is done as an added security feature in the Blu-ray format. For example, when analyzing a Blu-ray video disc, the flag indicates whether the BD-ROM drive will transfer encrypted data to the EclipseSuite tools. If the flag is set, this means that the EclipseSuite tools have to un-encrypt the data prior to analyzing it. Currently, the drives transfer un-encrypted data.

NOTE
Currently, there are less than a handful of BD-ROM drives that support Bus Encryption and all of these drives are for laptop computers. However, starting in July 2011, the specifications require that new drives must support Bus Encryption.

In a BDCMF image, Bus Encryption is specified in the User Control Data file (UCD.DAT) and in the Content Certificate file(s) inside the User Data file (UD.DAT). Therefore, it is easy for the EclipseSuite tools to analyze and detect any inconsistency. On a disc, however, the User Control Data area is inaccessible. Therefore, only the Content Certificate file(s) can be checked to see if the Bus Encryption Flag is enabled.

Severity

This rule does not identify a problem. Bus Encryption is part of the Blu-ray specifications and it is fully supported by the EclipseSuite tools. However, be aware that there are no drives available for testing Bus Encryption. Therefore, this rule is set as a 'Flag' severity to alert users of this fact. It is expected that this rule will be triggered in most images since Bus Encryption is currently not used.

Cause

The Bus Encryption flag is specified during authoring of an image. Since the use of this feature is relatively new and there are no drives available to support it, authors tend not to use it. Note also that not all authoring systems may support it either.

Solution

There is nothing users need to do if this rule is triggered unless Bus Encryption is required.

Type:	Exclude
Reference:	Blu-ray AACS Specifications
Default Program Action:	Flag

Rule ID: 1853

Bus Encryption enabled

This is an informational rule that specifies whether the Bus Encryption Enabled (BEE) flag IS SET in the Content Certificate file(s).

Background

The Bus Encryption Enabled flag indicates whether a player should transfer encrypted data to an application. This is done as an added security feature in the Blu-ray format. For example, when analyzing a Blu-ray video disc, the flag indicates whether the BD-ROM drive will transfer encrypted data to the EclipseSuite tools. If the flag is set, this means that the EclipseSuite tools have to un-encrypt the data prior to analyzing it. Currently, the drives transfer un-encrypted data.

NOTE
Currently, there are less than a handful of BD-ROM drives that support Bus Encryption and all of these drives are for laptop computers. However, starting in July 2011, the specifications require that new drives must support Bus Encryption.

In a BDCMF image, Bus Encryption is specified in the User Control Data file (UCD.DAT) and in the Content Certificate file(s) inside the UD.DAT file. Therefore, it is easy for the EclipseSuite tools to detect any inconsistency. On a disc, however, the User Control Data area is inaccessible. Therefore, only the Content Certificate file(s) can be checked to see if the Bus Encryption Flag is enabled.

Severity

This rule does not identify a problem. Bus Encryption is part of the Blu-ray specifications and it is fully supported by the EclipseSuite tools. However, be aware that there are no drives available for testing Bus Encryption. Therefore, this rule is set as a 'Flag' severity to alert users of this fact. If this rule is triggered, special handling may be required in order to analyze the media.

Cause

The Bus Encryption flag is set during authoring of an image. Since the use of this feature is relatively new and there are no drives available to support it, authors tend not to use it. Note also that not all authoring systems may support it either.

Solution

If this rule is triggered during analysis of a Blu-ray image, you may require a BD-ROM drive that supports Bus Encryption in order to fully analyze the image. Contact Eclipse Support for further assistance.

Type:	Exclude
Reference:	Blu-ray AACS Specifications
Default Program Action:	Flag

Rule ID: 1852

Bus Encryption not verified

The drive being used to analyze the Blu-ray disc does not support Bus Encryption.

Background

Bus encryption is another layer of data protection. Flags can be set to indicate whether the data transferred between a drive and host PC will be encrypted. However, this feature of the Blu-ray format is not commonly used primarily because it is new and there are no drives that support it.

This rule is triggered when a Blu-ray disc is identified as having the Bus Encryption Flag(s) enabled. However, the drive being used to analyze the disc does not support Bus Encryption. This should not affect the analysis of the media but the EclipseSuite tools will not be able to validate the Bus Encryption.

Severity

This rule is considered a WARNING since the Bus Encryption cannot be validated.

Cause

This condition occurs when analyzing a Blu-ray disc that has the Bus Encryption flag(s) set but a drive that does not support Bus Encryption is being used.

Solution

Try using a drive that supports Bus Encryption in order to get a full analysis of the image. Contact Eclipse Customer Support for further assistance.

NOTE

Currently, there are less than a handful of BD-ROM drives that support Bus Encryption and all of these drives are for laptop computers. However, starting in July 2011, the specifications require that new drives must support Bus Encryption.

Type:	Exclude
Reference:	Blu-ray AACS Specifications
Default Program Action:	Warning

Rule ID: 1856

Cannot copy AACS encrypted disc

This error occurs when trying to perform an ImageCopy operation of an AACS-encrypted Blu-ray disc.

Background

AACS is the standard encryption used on Blu-ray. If a replica has AACS copy protection applied then you cannot make copies of it.

Type:	Other
Reference:	None
Default Program Action:	Error

Rule ID: 848

Cannot determine 3D Base and Dependent Clip

The EclipseSuite tools cannot determine if a Clip AV Stream file is the Base view or Dependent View.

Background

The video output on a 3D Blu-ray Video image is composed of base view and dependent view for the left eye and right eye respectively. The specifications allow the data for both to be interleaved within the same Clip AV file or in separate Clip AV files. For each Clip AV Stream file there is a matching Clip Info file that describes the Clip AV Stream file. The Clip Info file includes data that identifies the Clip AV Stream file as being part of a 3D video stream. Similarly, a 3D PlayList will identify the base and dependent view clip files.

This error indicates that the Clip Info or 3D PlayList did not provide any information about a Clip AV Stream file. Therefore, the EclipseSuite tools are not able to determine if the clip is the Base or Dependent view.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display more details.

Severity

This rule is considered an ERROR since it may indicate that the image is authored incorrectly.

Cause

This condition is caused by the authoring system that created the image.

Solution

Contact the author of the image or Eclipse Customer Support for further assistance.

Type:	3D-BD
Reference:	N/A
Default Program Action:	Error

Rule ID: 1876

Can't trust BD-J application

A BD-Java application can't be authenticated and, therefore, cannot be trusted.

Background

BD-Java applications and related files are stored in JAR files inside the JAR directory. The META-INF directory inside a JAR file includes the Manifest, Signature and Signature Block files. The Manifest file includes a hash for each file inside the JAR file. The Signature file has a similar structure as the Manifest file. However, the Signature file includes a hash for each file entry in the Manifest file. It also includes a hash for the whole Manifest file. The Signature file is signed and its signature is stored in a certificate inside the Signature Block file.

Since it is possible to have multiple signers, each signer will have a matching Signature/Signature Block file pair. To support multiple signers, the file naming convention is as follows:

Signature file: **SIG-BDxx.SF**
Signature Block File: **SIG-BDxx.RSA**

The **xx** is an identifier to distinguish one file from another, thus, allowing multiple Signature/Signature Block files. The **xx** portion of the files starts from '00' and increment sequentially. A matching Signature/Signature Block file pair must have a matching **xx** identifier.

This error occurs when a Signature/Signature Block file pair is not found on the image. Therefore, a BD-J Application cannot be authenticated and, therefore, can't be trusted.

Additional Info

When this error occurs, the **Additional Info** column in the Analysis will display more details with the following message.

'[*BDJOFile*]' [*AppID*], '[*JARFile*]', ([*SigFileID*]) **SF/SBF pairs**

This message identifies the BD-J Object file being analyzed when this error occurred. The BD-J Object file contains a list of all BD-Java applications and the JAR file where they are stored. Each BD-Java Application is identified by a unique ID (AppID). Inside the JAR file, the Signature and Signature Block files contain hashes and digital signature for the BD-Java applications and related files. Since there could be multiple signers, the SigFileID identifies the Signature and Signature Block file pair that the EclipseSuite tools were analyzing. This error condition indicates that only one of the two files (Signature or Signature Block file) or neither was found.

Severity

If either the Signature, Signature Block, or both files are missing, then BD-Java applications cannot be authenticated and, therefore, cannot be trusted. This is considered an ERROR.

Cause

This problem typically occurs in authoring of the image.

Solution

The image must be re-authored.

Type:	Blu-ray

Reference:	Blu-ray Specifications, Section 3-2: BD-Java Specifications
Default Program Action:	Error

Rule ID: 1632

Can't trust JAR included file

One of the files inside a JAR file failed authentication. Therefore, it cannot be trusted.

Background

The JAR Manifest file inside a JAR file includes entries; one for each file inside a JAR file. Each entry includes the filename and a SHA-1 Digest for the file. During the analysis of the JAR Manifest file, the EclipseSuite tools will recalculate the digest for each file and compare the recalculated value to the file's SHA-1 digest in the JAR Manifest File. This error indicates that a SHA-1 Digest did not match the recalculated value; indicating that the file was altered or corrupted.

Additional Info

When this error occurs, the **Additional Info** column in the Analysis will display more details with the following message.

'[*JARFile*]', '[*JARManifestFile*]', '[*Filename*]', ([*FileSize*]) byte(s) digest '[*DigestValue*]'

This message identifies the JAR file, JAR Manifest file and the file which failed authentication. The file's size and digest value are also displayed.

Severity

This rule indicates that a file may have been altered or is corrupt. Therefore, it is considered an ERROR.

Cause

This problem typically occurs in authoring of the image.

Solution

The image must be re-authored.

Type:	Blu-ray
Reference:	Blu-ray Specifications, Section 3-2: BD-Java Specifications
Default Program Action:	Error

Rule ID: 1638

Can't trust JAR Manifest file

The JAR Manifest File cannot be authenticated or failed authentication. Therefore, it cannot be trusted.

Background

The Signature File includes a digest for the JAR Manifest File. If the Signature File fails authentication, then the JAR Manifest File cannot be authenticated. If the Signature File passes authentication, the Digest for the JAR Manifest File can be recalculated then compared to the digest in the Signature File. If they do not match, then the JAR Manifest File fails authentication.

Additional Info

When this error occurs, the **Additional Info** column in the Analysis will display more details with the following message.

'[*BDJObjectFile*]' [*AppID*], '[*JARFile*]', '[*SignatureFile*]','[*JARManifestFile*]'

This message identifies the Signature File failed authentication. Since the Signature file is the only one that can authenticate the JAR Manifest file, then the JAR Manifest File itself cannot be trusted.

'[*JARFile*]', '[*SignatureFile*]','[*JARManifestFile*]', ([*FileSize*]) **byte(s), digest** '[*DigestValue*]'

This message indicates that the JAR Manifest file failed authentication. The Signature File holds a Digest for the JAR Manifest File. During analysis of the Signature File, the EclipseSuite tools validated the digest for the JAR Manifest file and it failed.

Severity

This rule indicates that a file may have been altered or is corrupt. Therefore, it is considered an ERROR.

Cause

This problem typically occurs in authoring of the image.

Solution

The image must be re-authored.

Type:	Blu-ray
Reference:	Blu-ray Specifications, Section 3-2: BD-Java Specifications
Default Program Action:	Error

Rule ID: 1641

Can't trust JAR Manifest file entry

A file entry in the JAR Manifest file has failed authentication.

Background

The JAR Manifest File includes entries for each file in a JAR file. Each entry includes a filename and a SHA-1 digest for the file. Each entry (filename & digest) is hashed and stored in another entry inside the Signature File. During analysis of the Signature File, the EclipseSuite tools recalculate the digest for each file entry in the JAR Manifest File and compare the result with the digest in the matching entry in the Signature File. If they do not match, then this error is triggered.

Additional Info

When this error occurs, the **Additional Info** column in the Analysis will display more details with the following message.

'[*JARFile*]', '[*SignatureFile*]', '[*Filename*]', ([*FileSize*]) byte(s), digest '[*DigestValue*]'

This message identifies the filename entry that failed authentication.

Severity

This rule indicates that a file may have been altered or is corrupt. Therefore, it is considered an ERROR.

Cause

This problem typically occurs in authoring of the image.

Solution

The image must be re-authored.

Type: Blu-ray
Reference: Blu-ray Specifications, Section 3-2: BD-Java Specifications
Default Program Action: Error

Rule ID: 1642

Can't trust JAR Signature file

The Signature Block file failed authentication. Since the Signature File can only be authenticated by the Signature Block File, then it can't be authenticated either. Therefore, it cannot be trusted.

Background

The Signature Block File contains certificates that can authenticate the Signature Block file. This error indicates that the Signature Block File failed authentication. Therefore, the Signature file cannot be authenticated and, therefore, cannot be trusted.

Additional Info

When this error occurs, the **Additional Info** column in the Analysis will display more details with the following message.

'[*BDJObjectFile*]' [*AppID*], '[*JARFile*]', '[*SignatureFile*]'

This message identifies the Signature file that failed authentication.

Severity

This is considered an ERROR since it indicates that the Signature Block file has been altered or is corrupt.

Cause

This problem typically occurs in authoring of the image.

Solution

The image must be re-authored.

Type: Blu-ray
Reference: Blu-ray Specifications, Section 3-2: BD-Java Specifications

Default Program Action: Error

Rule ID: 1644

Can't trust TBS certificate

Authentication of a certificate failed. Therefore, the certificate can't be trusted.

Background

To validate that BD-Java applications and related files have not been compromised, authors provide a digital signature in certificates inside the Signature Block File. The EclipseSuite tools analyze all certificates and their digital signatures to make sure they match the BD-Java content on the image.

The Signature Block File includes a certificate chain starting with the application root certificate and ending with the leaf certificate that contains the digital signature that is used to authenticate the BD-Java content. As part of the BD-Java Security Analysis, the EclipseSuite validate the certificate chain.

When a tbsCertificate is signed, it is encrypted with the private key of the issuer who is issued the certificate. The signature value is stored in the certificate's signature value field. When validating the signature, the signature is re-generated using the key from the previous (parent) certificate. If the resulting value is not equal to the one stored in the signature value field, then this error occurs.

Additional Info

When this error occurs, the **Additional Info** column in the Analysis will display more details with one of the following messages.

'[*JARFile*]', '[*SignatureBlockFile*]': cert([*SerialNo*] | [*CertIdx*]), Issuer: '[*Issuer*]'

This message identifies the JAR file and Signature Block file that are being analyzed. The Signature Block File contains the certificates that are being analyzed. The Serial Number, Certificate Index and Issuer fields identify the certificate that failed authentication.

'disc root', '[*RootCertFilename*]': cert([*SerialNo*] | -1), Issuer: ''

This message identifies the root certificate as the one that failed authentication.

Severity

The application root certificate is required for authentication of the BD-Java content. Therefore, this is considered an ERROR.

Cause

This problem typically occurs in authoring of the image.

Solution

The image must be re-authored.

Type:	Blu-ray
Reference:	Blu-ray Specifications, Section 3-2: BD-Java Specifications
Default Program Action:	Error

Rule ID: 1630

CC Bus Encryption Enabled flag not set

The Bus Encryption Enabled (BEE) flag is not set on the Layer 1 Content Certificate file.

Background

The specifications require that both Content Certificate files in a dual-layer BD image reflect the same bus encryption status. In this case, this error indicates that bus encryption was set on the Layer 0 Content Certificate file but not on the Layer 1 Content Certificate file.

Severity

This condition is considered an error since it is possible that it may lead to playability problems.

Cause

This problem is typically caused by the authoring application.

Solution

The image must be re-authored. Contact Eclipse Customer Support for further assistance.

Type:	Blu-ray
Reference:	Blu-ray AACS Specifications
Default Program Action:	Error

Rule ID: 1854

CC Order Delivery File and calculated CC mismatch

The Content Certificate Order Delivery File and the calculated Content Certificate file do not match.

Background

A Content Certificate Order Delivery File is the signed content certificate files that are returned from AACS LA. These files are used by the CMU utility to create a Type AX image using the original Type A, Type B image and this CC Order Delivery Files. During the creation of the Type AX image, the CC Order Delivery Files are renamed to ODFL0.DAT for layer 0 and ODFL1.DAT for layer 1. During the analysis of a Type AX image, the EclipseSuite tools will re-create the Content Certificate file in memory then compare it to the CC file included with the image (ODFLx.DAT, where x = layer#). If they are not the same, then this rule is triggered.

The EclipseSuite tools also check the size of the CC Order Deliver File to make sure it is the correct size. Space for the CC was reserved when the image is first authored. The size of the calculated CC should not be longer than the amount of space reserved.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display more details with one of the following messages.

'ODFL0.DAT' size is bigger than calculated '[*filename*]'

This message indicates that the size of the layer 0 CC file is greater than the calculated CC file. This indicates that possibly the wrong CC file was included with the image.

The size of the CC file is determined and reserved during authoring of the image. When the image is converted from Type A to Type B, the Content Certificate file in the image is filled with Digests from hashes from all AVClip files. The CC for each layer is then extracted and submitted to AACS LA for signing. When creating a Type AX image using the signed CC, original Type A image and encrypted Type B image, the CMU copies the signed CC files to the Type AX image directory and renames them ODFL0.DAT and ODFL1.DAT. The files must not be longer than the space that was originally reserved for them in the image.

This message indicates that the CC file for layer 0 (ODFL0.DAT) is larger than the space originally reserved. This might indicate that the wrong order file was selected when the Type AX image was created.

'ODFL1.DAT' size is bigger than calculated '[filename]'

This message indicates that the size of the layer 1 CC file is greater than the calculated CC file. This indicates that possibly the wrong CC file was included with the image.

The size of the CC file is determined and reserved during authoring of the image. When the image is converted from Type A to Type B, the Content Certificate file in the image is filled with Digests from hashes from all AVClip files. The CC for each layer is then extracted and submitted to AACS LA for signing. When creating a Type AX image using the signed CC, original Type A image and encrypted Type B image, the CMU copies the signed CC files to the Type AX image directory and renames them ODFL0.DAT and ODFL1.DAT. The files must not be longer than the space that was originally reserved for them in the image.

This message indicates that the CC file for layer 1 (ODFL1.DAT) is larger than the space originally reserved. This might indicate that the wrong order file was selected when the Type AX image was created.

'ODFL0.DAT' and calculated '[*filename*]'

This message indicates that the layer 0 CC file (ODFL0.DAT) does not match with the calculated CC file created during the analysis of the image.

The size of the CC file is determined and reserved during authoring of the image. When the image is converted from Type A to Type B, the Content Certificate file in the image is filled with hashes from all encrypted AVClip files. The CC for each layer is then extracted and submitted to AACS LA for signing. When creating a Type AX image using the signed CC, original Type A image and encrypted Type B image, the CMU copies the signed CC files to the Type AX image directory and renames them ODFL0.DAT and ODFL1.DAT. During the analysis of an AX image, the EclipseSuite tools re-generate the CC in memory and at the end of the job compare the calculated CC to the CC file included with the image (ODFL0.DAT). If they are not the same, then this rule is triggered.

This might indicate that the wrong order file was selected when the Type AX image was created.

'ODFL1.DAT' and calculated '[*filename*]'

This message indicates that the layer 0 CC file (ODFL0.DAT) does not match with the calculated CC file created during the analysis of the image.

The size of the CC file is determined and reserved during authoring of the image. When the image is converted from Type A to Type B, the Content Certificate file in the image is filled with hashes from all encrypted AVClip files. The CC for each layer is *then extracted and submitted to AACS LA for signing. When creating a Type AX image using the signed CC, original Type A image and encrypted Type B image, the CMU copies the signed CC files to the Type AX image directory and renames them ODFL0.DAT and ODFL1.DAT. During the analysis of an AX image, the EclipseSuite tools re-generate the CC in memory and at the end of the job compare the calculated CC to the CC file included with the image (ODFL1.DAT). If they are not the same, then this rule is triggered.*

This might indicate that the wrong order file was selected when the Type AX image was created.

Severity

This rule is considered an error since it indicates that possibly the wrong CC files were included with the image. It may not be possible to process this image.

Cause

Type AX images were new as of BDCMF 0.97. This rule was added as a precaution to make sure that if the CC files are mixed up, the EclipseSuite tools can detect it and warn the user. If this condition occurs, it is likely caused by the wrong CC being selected during the conversion to Type AX.

Solution

Since it is likely that the wrong CC files were selected, it is recommended that the Type AX image be created again and confirm that the correct CC Order Delivery File is being selected.

Contact Eclipse Customer Support for further assistance.

Eclipse Customer Support
Phone: (925) 598-0300
Email: Support@eclipsedata.com

Type:	Blu-ray
Reference:	BDCMF Specifications Version 0.97 and later
Default Program Action:	Error

Rule ID: 1531

CC/UCD Bus Encryption Flag Mismatch

The encryption flag in the Content Certificate does not match the Bus Encryption Flag in the User Control Data.

Background

Each Content Certificate includes the bit flag 'Bus Encryption Enabled' (BEE) which indicates whether or not the data covered by the Content Certificated is encrypted when being transferred between a drive and host PC.

The User Control Data (UCD.DAT) consists of 18 bytes for each sector of user data. Bit #7 of the first byte is the Bus Encryption Flag (BEF). This flag is used to indicate whether the user data of a sector should be encrypted between the drive and host PC.

When an image is flagged for Bus Encryption, all video files under the \BDMV\STREAM directory will be encrypted when transferred between a drive and host PC. When this flag is set in the CC, the Copy_permission_indicator (CPI) bits in the Aligned Units covered by the CC must be set to 112.

This rule is triggered when the BEE and BEF flags and sector encryption status don't agree.

> **NOTE**
> *The use of Bus Encryption flag has been supported since BDCMF 1.10. However, hardware support has not been implemented yet. The Blu-ray specifications require that new drives manufactured starting July 1, 2011 must support Bus Encryption.*

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display the following message.

UCD: [*Enabled/Disabled*], **Sector:** [*Encrypted/Unencrypted*], **CC:** [*Enabled/Disabled*]

This message indicates that one of the following conditions occurred:

- *BEE = 1, BEF = 0, CPI = 01, 10 or 11*

  The bus encryption status specified by the BEF flag in the User Control Data (UCD.DAT) does not match the BEE flag and CPI bits.

- *BEE = 0, BEF = 1, CPI = 01, 10 or 11*

  The bus encryption status specified by the BEE flag in the Content Certificate does not match the BEF and CPI bits.

- *BEE = 1, BEF = 1, CPI = 00*

  The CPI bits in an Aligned Unit do not match the BEF flag in the UCD. The UCD includes a BEF flag for each sector. It is unknown whether the UCD or the CPI bits are incorrect.

Severity

Inconsistencies in the bus encryption may cause playability problems. Therefore, it is considered an ERROR.

Cause

This problem is typically caused during authoring of the image.

Solution

The image may need to be re-authored. Contact Eclipse Customer Support for further assistance.

Type:	Blu-ray
Reference:	AACS Specifications
Default Program Action:	Error

Rule ID: 1672

Checksum differs

The re-calculated checksum for a BDCMF file is different from the original value.

Background

When a Blu-ray image is processed using ImageCopy, a checksum file will be created where checksums for each file of the BDCMF file-set will be stored. As the image is processed in the pre-mastering and mastering environments using the EclipseSuite tools, some of the image files will be altered and the checksums are updated to reflect those changes. There are conditions that may cause the updating of the checksums to fail. This results in checksum differences the next time the image is analyzed.

This rule was introduced to distinguish between checksum errors that occur in the user data files and the other BDCMF files. This rule will be triggered when the checksum fails for one of the BDCMF files (e.g. AACS1.DAT, PIC.DAT, etc.). The original rule "File Checksum error" will be triggered if the checksum for the user data file (e.g. UD.DAT) fails.

Additional Info

When this rule is triggered, the **Additional Info** column will identify the file whose checksum failed.

[*Filename*] **- See Info/Checksums**

This message identifies the file whose checksum failed. You can view the checksums by clicking on the Info tab then on the ChckSum button.

Severity

This rule is considered a WARNING since it is only triggered for the BDCMF files and not the user data files. However, you should still try to determine the cause of the checksum differences.

Cause

This type of problem typically occurred during the signing of an image using Eclipse's CMU utility or during the mastering process. When the image is signed, there are several files that are altered. The CMU utility must make these changes and update the checksums. If a problem occurs that causes the CMU not to update the checksums then it will cause this rule to be triggered the next time the image is analyzed. Similarly, when the image is mastered, some files will be altered and the encoder must update the checksums.

Solution

There have been several enhancements to prevent this condition from happening. Previously, the error "File Checksum error" was triggered for any checksum failure. Since this condition only affected files that did not contain user data and these there was nothing actually wrong with these files, this rule was introduced to identify this condition and allow operators to continue. However, be aware that this rule can also be triggered if a file becomes corrupt. If the file is corrupt, other errors may be triggered.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Warning

Rule ID: 1560

Clip assigned to a CPS Unit

This Blu-ray warning indicates that there is an orphaned clip on the media and that the Eclipse tools have assigned the orphaned clip to a CPS Unit.

Background

During the analysis of a Blu-ray image, the Eclipse software parses through the PlayList to identify the encryption keys used for the video clips. This is required for decryption and analysis, and is done in much the same way a player would play a disc. In some cases, video files are contained on the media that are not referenced by a PlayList. When this occurs, the Eclipse software cannot be sure which encryption key should be used to decrypt the clip and the software must assign the clip to a CPS Unit in order to proceed. Typically this warning is triggered only on replicas and will not be seen during ImageCopy AACS encryptio operation, or ImageAnalysis of an image file. When working with image files, the EclipseSuite tools rely on instructions in the BDCMF file-set to identify the CPS Unit of each clip rather than on the PlayList reference.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will identify the Clip AV file and th CPS Unit number it assigned to it.

[*filename*] **forced to CPSUnit (clip unit)**

This message shows the orphaned filename and the clip number that it was assigned by the Eclipse software.

Possible Cause

This warning is triggered whenever the Eclipse tools find an orphaned clip. Orphaned clips are created whenever the authoring studio includes video that is not referenced in a PlayList either intentionally or unintentionally. This can be the result of advanced features such as online content or BD-J or a mistake in the PlayList programming.

Severity

When the Eclipse tools encounter orphaned clips, the software will assign the clip to the highest CPS Unit encountered on the disc. This will trigger this rule message which should accompany each instance of the "Clip AV Stream not assigned to a CPS Unit" error. In most cases, the assigning of the CPS Unit key will result in successful decryption. ImageVerify of such a title to the original source should show no comparison errors, indicating that the disc matches the source and has been encrypted correctly.

This warning is acceptable as long as:

- ImageVerify between the source and the replica shows that the title has no comparison errors.
- An instance of "Clip assigned to a CPS Unit" is found for each "Clip AV Stream not assigned to a CPS Unit" error.

Type:	Blu-ray
Reference:	Blu-ray specifications for read-only media
Default Program Action:	Warning

Rule ID: 1469

Clip AV Stream file size not an AU boundary

A Clip AV file does not end with an Aligned Unit.

Background

A Clip AV file consists of an integer number of Aligned Units, where each Aligned Unit consists of 3 logical sectors (32 source packets). Therefore, the file size must be an integer number of Aligned Units. When the last Aligned Unit is not completely filled with audio/video information, the remaining source packets are filled with Null values.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will identify the Clip file that triggered this rule.

File [*#####.m2ts*], length [*FileSize*]

This message identifies the Clip file (.m2ts) and its file size.*

Severity

It is unknown if this condition causes any problems. However, it is a violation of the Blu-ray specifications. Therefore, it is considered an ERROR.

Cause

This problem is caused by the authoring system that created the image.

Solution

This problem cannot be corrected in the pre-mastering or mastering process. The image must be re-authored.

Type:	Blu-ray
Reference:	Blu-ray Disc Read-Only Format Part 3: Audio Visual Basic Specifications
Default Program Action:	Error

Rule ID: 1585

Clip AV Stream in different CPS Units

This Blu-ray message indicates that the same Clip AV Stream file is specified with more than one CPS Unit.

Background

A CPS Unit key refers to a title key that is used for encryption. All Titles have references to Clip AV Stream files. A Clip AV Stream file must be encrypted with the same CPS Unit Key as the title that references it. This rule indicates that a Clip AV Stream file is referenced by more than one Title which are encrypted with different CPS Unit keys.

Additional Info

When this error is triggered, the **Additional Info** column in the analysis will identify the Clip AV Stream file and the CPS Unit numbers in question with the following message.

Clip '[*filename*]', CPS Units ([*CPSUnit No*]) and ([*Other CPSUnit No*])

This message identifies the Clip AV filename (.m2ts) and the two CPS Unit numbers that reference it.*

Error Severity

This error indicates that there is more than one reference to the same Clip AV file by different Titles that are encrypted with different CPS Unit keys. This is considered an error since it is unknown as to which of the title keys was used to encrypt the file.

Possible Cause

This problem is typically introduced when the image is created.

Possible Solution

If the problem occurs on a source BDCMF image, then it may be possible to correct this error by manually editing the BDCMF.CMF file. However, you must be familiar with the CMF specifications and know where the changes need to be made.

If editing is not possible, then the image must be re-authored.

Type:	Blu-ray
Reference:	AACS Blu-ray Pre-recorded Book Revision 0.92
Default Program Action:	Error

Rule ID: 839

Clip AV Stream mapping is incorrect

A Clip file was encrypted with the wrong CPS Unit.

Background

During analysis of an encrypted image (including a replicated disc), the EclipseSuite tools must first determine the encryption keys that were used to encrypt the Clip AV files in order to decrypt and analyze them. While a CPS Unit specifies an encryption key, each Clip AV file has references back to a specific CPS Unit. Once it is determined which CPS Unit a Clip AV file belongs to, then it can be decrypted and analyzed. However, there are cases in which Clip AV files were decrypted with the right key but analyzed as being corrupt. When this happens, the EclipseSuite tools try using all other encryption keys (if any) and see if using any of them can successfully decrypt the file. If any other key is successful, then this error is triggered, indicating that the file was encrypted with the wrong key.

Additional Info

When this rule is triggered, the **Additional Info** column in the analysis will display the following message.

'[*ClipAVFile*]' moved from CPS Unit ([*OldCPSUnitNumber*]) to ([*NewCPSUnitNumber*]) for analysis

This message identifies the Clip AV file (.m2ts) which has been encrypted with the wrong key. It also identifies that CPS Unit number that it belongs to (OldCPSUnitNumber) and the CPS Unit that was used to encrypt it.*

Each Clip AV file belongs to a CPS Unit. Each CPS Unit specifies the key that is used to encrypt all Clip AV files belonging to that CPS Unit.

Severity

This rule is considered an ERROR since it is likely to cause playability problems.

Cause

This problem is typically caused by the utility that was used to encrypt the image (or Clip AV file).

Solution

The only solution is to re-encrypt the image. Contact Eclipse Support for further assistance.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

Rule ID: 1551

Clip AV Stream not assigned to a CPS Unit

This Blu-Ray error indicates that there is a clip on the media that is not referenced by a PlayList. In the EclipseSuite software, these files are referred to as "orphaned" clips.

This error is often found in conjunction with the warning "Clip assigned to a CPS Unit".

Background

During the analysis of a Blu-ray image, the Eclipse software parses through the PlayList to identify the encryption keys used for the video clips. This is required for decryption and analysis and is done in much the same way a player would play a disc. In some cases, video files are contained on the media that are not referenced by a PlayList. When this occurs, the EclipseSuite software cannot be sure which encryption key should be used to decrypt the clip and the error is reported. Typically this error is identified only on replicas and will not be seen during ImageCopy AACS encryption operation, or ImageAnalysis of an image file. When working with image files, the EclipseSuite tools rely on instructions in the BDCMF file set to identify the CPS Unit of each clip rather than on the PlayList reference.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will identify the Clip AV stream file.

Blu-ray Video: '[*filename*]'

This message identifies the clip filename in question.

Possible Cause

This error is triggered when authoring studio includes video that is not referenced in a PlayList either intentionally or unintentionally. This can be the result of advanced features such as online content, BD-J or a mistake in the PlayList programming.

Severity

Although this is considered an error, orphaned clips are not uncommon. When the EclipseSuite tools encounter this error, the software will assign the clip to the highest CPS Unit encountered on the disc. This is reported with the warning message "Clip assigned to a CPS Unit" which should accompany each instance of this error. In most cases, the assigning of the CPS Unit key will result in successful decryption. A verification of such a title to the original source should not result in comparison errors, indicating that the disc matches the source and has been encrypted correctly.

This error is acceptable as long as:

- ImageVerify shows that the title has no comparison errors.
- An instance of "Clip assigned to a CPS Unit" is found for each orphaned clip.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

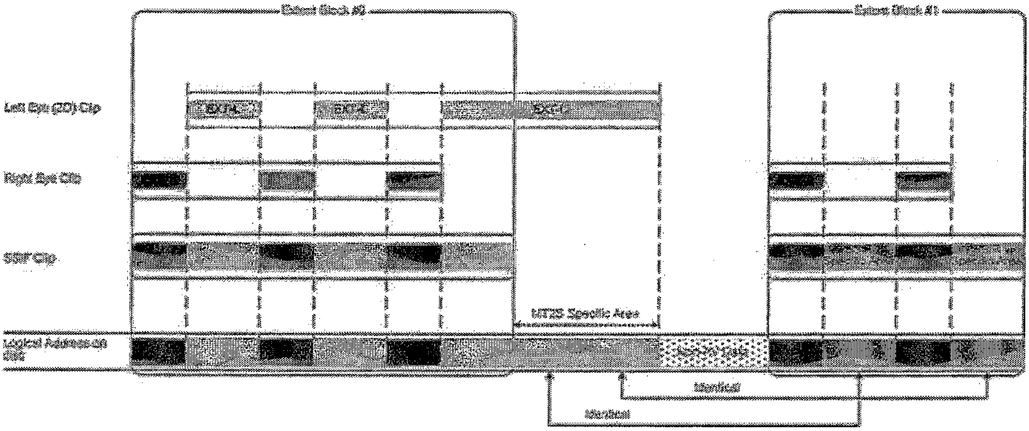
Rule ID: 853

Clip common area not a multiple of an Aligned Unit

The Blu-ray specifications for 3D require that Common Area length be a multiple of an Aligned Unit.

Background

A 3D image has data for the left and right eye. Normally, the left and right eye data are stored in separate Clip AV files. The Extents from these two files are mapped into a stereoscopic interleaved file (SSIF). Some areas of the left file are not mapped into the SSIF. These are referred to as M2TS Specific Areas. Similarly, the SSIF file includes areas that are not part of the left eye file. These areas are referred to as SSIF Specific Areas. The 3D specifications require that the length of the Specific Areas be a multiple of an Aligned Unit.



Severity

This condition defaults to an ERROR since it does not meet the 3D specification requirements.

Cause

This condition is caused by the authoring application that created the image.

Solution

The image must be re-authored. Contact Eclipse Customer Support for further assistance.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Info

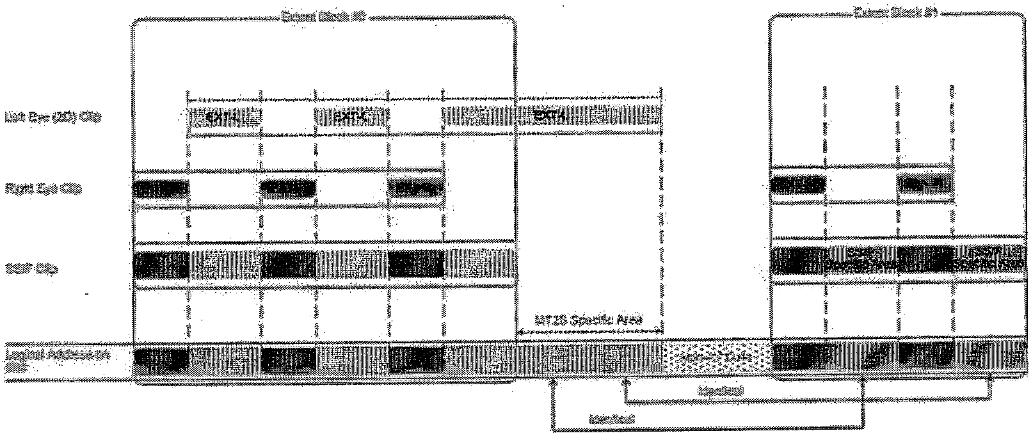
Rule ID: 1867

Clip specific area not a multiple of an Aligned Unit

The Blu-ray specifications for 3D require that Specific Areas length be a multiple of an Aligned Unit.

Background

A 3D image has data for the left and right eye. Normally, the left and right eye data are stored in separate Clip AV files. The Extents from these two files are mapped into a stereoscopic interleaved file (SSIF). Some areas of the left file are not mapped into the SSIF. These are referred to as M2TS Specific Areas. Similarly, the SSIF file includes areas that are not part of the left eye file. These areas are referred to as SSIF Specific Areas. The 3D specifications require that the length of the Specific Areas be a multiple of an Aligned Unit.



Severity

This condition defaults to an ERROR since it does not meet the 3D specification requirements.

Cause

This condition is caused by the authoring application that created the image.

Solution

The image must be re-authored. Contact Eclipse Customer Support for further assistance.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

Rule ID: 1866

Clip Stream not aligned at layer break

A Clip file spans into layer 1 but the total size of the file that is recorded on layer 0 is not a multiple of a Hash Unit (e.g. 32 logical sectors).

Background

The specifications require that if a Clip file spans between layers, the layer break point should occur at the end of a Hash Unit. In other words, a Hash Unit cannot be broken between layers.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will identify the file that spans between layers.

File [*Filename*], layer 0 size (*Size*) not a hash unit multiple

The file identified by this message spans layers. The portion recorded on layer 0 is not a size that is a multiple of a hash unit (32 sectors).

Fle *nnnnn*.m2ts layer 0 segment is too small

The Clip AV Stream file identified by this message spans layers. The portion that is recorded on layer 0 is smaller than a hash unit (32 sectors).

File *nnnnn*.m2ts

The Clip AV Stream file identified by this message spans layers. The portion recorded on layer 0 is not a size that is a multiple of a hash unit (32 sectors).

Severity

It is unknown if this condition will cause any problems. However, it is a requirement of the AACS specifications and, therefore, considered an ERROR.

Cause

This problem is caused by the authoring application that created the image.

Solution

The image must be re-authored.

Type:	MainChannel
Reference:	AACS Specifications

Default Program Action: Error

Rule ID: 880

ClipInfo file requires Extent_Start_Point() definition

The ExtensionData structure in the ClipInfo file does not include an Extent_Start_Point structure.

Background

The ExtensionData structure is used in Blu-ray Video to specify additional information used in the files index.bdmv, MovieObject.bdmv, xxxxx.mpls, zzzzz.clpi and sound.bdmv. There are different types of information that can be specified. Each entry in this data structure includes two fields that identify the data type that it represents.

In the case of a 3D image, the SSIF file is composed from extents derived from two two ClipAV Stream files (Base and Dependent Clips). The extents from the two ClipAV files are interleaved in the SSIF file. The ClipInfo (*.clpi) file for each of the ClipAV Stream files must include an Extent_Start_Point structure to specify the location of each interleaved segment of each ClipAV Stream file.

This error indicates that a ClipInfo file did not include ExtensionData specifying an Extent_Start_Point data structure.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will identify the ClipInfo file that is missing this information.

Severity

In order to display the proper 3D effect, it is required that the Base and Dependent Clips be interleaved in the SSIF file. Without the Extent_Start_Point data, it would be impossible for a player to know where the extents for the Base and Dependent views are located. It is likely that this will affect playability. Therefore, it is considered an ERROR.

Cause

This condition is caused by the authoring system that created the image.

Solution

The image must be re-authored. Contact Eclipse Support for further assistance.

Type: 3D-BD
Reference: 3D Specifications
Default Program Action: Error

Rule ID: 1760

ClipInfo file structural error

The EclipseSuite tools detected errors while analyzing a ClipInfo file.

Background

Part of the analysis of a Blu-ray Video image includes analysis of the contents of Clip Information files (zzzzz.clpi). ClipInfo files describe the contents of their corresponding Clip AV Stream files (zzzzz.m2ts). If during this analysis, the EclipseSuite tools find any errors then this rule is triggered.

ClipInfo Syntax	
Type Indicator	= 'HDMV'
Version	= '0200' or '0100'. It is recommended that version '0200' be used.
SequenceInfo Start Address	Start address of the SequenceInfo data structure.
ProgramInfo Start Address	Start address of the ProgramInfo data structure.
CPI Start Address	Start address of the CPI data structure.
ClipMark Start Address	Start address of the ClipMark data structure.
ExtensionData Start Address	Start address of the Extension data data structure.
SequenceInfo	
ProgramInfo	
CPI	
ClipMark	
ExtensionData	

Additional Info

When this rule is triggered, the **Additional Info** column in the analysis will display more details about the failure with one or more of the following messages.

Invalid type_indicator field in '[*ClipInfoFile*]'

The Type Indicator field must be set to 'HDMV'. This condition indicates that it is set to something else. Therefore, it is possible that this file may not be identified as a ClipInfo file.

Invalid version_number field in '[*ClipInfoFile*]'

The Version field must be set to either '0100' or '0200'. This condition indicates that it is not set to either of these two values. It is unknown how this may affect players.

Invalid memory access

This condition indicates an error processing the ClipInfo file.

Severity

All of the conditions listed above are considered serious and, therefore, this rule is an ERROR.

Cause

This condition is caused by the authoring system that created the image.

Solution

The image must be re-authored. Contact Eclipse Customer Support for further assistance.

Type:	Blu-ray
Reference:	Blu-ray Video Specifications
Default Program Action:	Error

Rule ID: 1759

CMF File Extent missing or incorrect

The UDF Allocation Descriptor Extents for a file do not match with the File Extents specified in the BDCMF.CMF file.

Background

The BDCMF Specifications require that all the Extents for certain files be specified in the BDCMF.CMF file. This Extent information specified in the BDCMF.CMF file must match with all of the file's UDF Allocation Descriptor Extents.

Additional Info

When this message is triggered, the **Additional Info** column in the analysis will identify the filename and the location of the Extent that is missing.

[*file name*], **expected** [*extent location*]

This message identifies the filename in question and the expected extent. The filename can be any of the following.

*\BDMV\STREAM\**
\AACS\CONTENTHASH001.TBL
\AACS\CONTENT000.CER
\AACS\CONTENTHASH000.TBL
\AACS\CONTENT001.CER
\AACS\CONTENTREVOCATION.LST
\AACS\MKB_RO.INF
\AACS\MKB_RW.INF
\AACS\UNIT_KEY_RO.INF
\AACS\SEGMENT_KEY.INF

Example:

```
<File Type="ClipAVStream" Name="00002.m2ts" Access="Extent" >
    <CPSUnitNo>1</CPSUnitNo>
    <Extent Start="10441737" Size="524256" />
    <Extent Start="10965993" Size="58080" />
</File>
```

Error Severity

This condition is considered serious since the extents are used during the encryption process. Without the extent information, it may not be possible to encrypt the file.

Possible Cause

This problem it typically introduced when the image is created.

Possible Solution

The EclipseSuite software is able to analyze and display all file information including all extents. Therefore, it may be possible to manually edit the BDCMF.CMF file to correct this condition. However, you must be familiar with the CMF specifications and know where the changes need to be made.

If editing is not possible, then the image must be re-authored.

Type:	Blu-ray
Reference:	UDF and BDCMF Specifications
Default Program Action:	Error

Rule ID: 1430

Common CPS Unit Key not available

An error occurred when trying to process the Common CPS Unit key.

Background

A CPS Unit Key, or Title Key, refers to an encryption key that is used to encrypt Clip files belonging to the same CPS Unit. Normally, the CPS Unit Keys are automatically generated by the encryption utilities, such as ImageCopy. However, BD-Live images require that the online content be encrypted with a CPS Unit Key that already exists in the image. To support this process, authoring studios will encrypt the online content with an encryption key determined by the authoring studio. When sending the image to be mastered, the studio provides the encryption key to the mastering facility so that it is used when the image is encrypted. Since the same key is used for the online content as well as the image, it is referred to as a 'Common CPS Unit Key'.

When using ImageCopy to encrypt an image, ImageCopy will identify the authoring studio that created the image. Once identified, ImageCopy will check to see if a 'Common CPS Unit Key' is available from this studio. If one is found, it will be used to encrypt all Clip files for the matching CPS Unit. This error is triggered if a problem occurs during this process.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display more details with one of the following messages.

CPS Unit [*CPSUnit*]. PGP installation required to process common CPS Unit keys for Movie Studio '[*MovieStudio*]'

This message indicates that PGP is not installed on the computer. Since the CPS Unit Key is PGP-encryted, PGP must be installed in order for ImageCopy to unencrypt it. Please ensure that PGP is installed before processing this image.

This message identifies the Movie Studio and the CPS Unit that ImageCopy is looking for.

CPS Unit [*CPSUnit*]. No 'CommonKeyFile' for Movie Studio '[*MovieStudio*]'

This message indicates that ImageCopy the MovieStudios.xml file does not include a CommonKeyFile attribute for the Movie Studio specified by this message. Therefore, there is no Common CPS Unit Key File that can be used for images from this studio. Contact Eclipse Support for further assistance.

CPS Unit [*CPSUnit*]. No 'Movie Studio common keys dir' preference specified

This message indicates that a directory has not been specified where the Movie Studio Common Keys can be found. This folder must be specified in the Copy Protection tab in the ImageCopy Preferences.

CPS Unit [*CPSUnit*]. Common key file '[*CommonKeyFile*]' not found

This message indicates that the file specified does not exist in the directory specified. The CommonKeyFile directory is specified in the Copy Protection tab in the ImageCopy Preferences.

CPS Unit [*CPSUnit*]. Failed to deploy PGP resource

This message indicates an internal program error when attempting to load PGP resources in order to process the Common CPS Unit Key file. Please contact Eclipse Support for further assistance.

CPS Unit [*CPSUnit*]. Failed to load resource data

This message indicates an internal program error when attempting to load program resources in order to process the Common CPS Unit Key file. Please contact Eclipse Support for further assistance.

CPS Unit [*CPSUnit*]. Failed to decrypt file '[*CommonKeyFile*]'

This message indicates that ImageCopy was unable to unencrypt the Common CPS Unit Key file.

CPS Unit [*CPSUnit*]. Can not get key from '[*CommonKeyFile*]'

This message indicates that ImageCopy was unable to read the CPS Unit Key from the Common CPS Unit Key File.

CPS Unit [*CPSUnit*]. No previous key in file '[*CommonKeyFile*]'

This message indicates that the Common CPS Unit Key file does not include the CPS Unit Key that ImageCopy is looking for.

Severity

It is possible that the image may not be processed correctly. Therefore, this is considered a WARNING.

Cause

Unknown.

Solution

Please contact Eclipse Support for further assistance.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Warning

Rule ID: 1677

Common CPS Unit Key was not used for encryption

******* The description of this rule is not available as it contains confidential information.*******

For more information, please contact Eclipse Customer Support.

Eclipse Customer Support

Phone: (925) 598-0300
Email: Support@eclipsedata.com

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Flag

Rule ID: 1817

Content Certificate File Hash Error

One of the hash values in the Content Certificate is incorrect.

Background

Hashes are used to validate the integrity of a file. During the encryption process of a Type A image (e.g. conversion from Type A to Type B), ImageCopy generates hash values for the Managed Copy Manifest File (\AACS\mcmf.xml), BD-J Root Certificate file (\CERTIFICATE\app.discroot.crt) and all CPS Usage files (\AACS\CPSUnitXXXXX.cci). The hash values are stored in the content certificate.

During analysis of a BD image that is already encrypted (including a disc), the EclipseSuite tools recalculate all hash values and compare them to the hash values stored in the content certificate. If any do not match, then this rule is triggered.

Severity

This condition indicates file corruption, which will likely affect playability. Therefore, it is considered an ERROR.

Cause

This problem can occur if an image becomes corrupt due to hard disk corruption. However, if is also possible that it can occur if the hashes are not calculated correctly when they are saved to the Content Certificate or during the analysis of a pre-encrypted image.

Solution

An image with this problem should not be used for mastering. Contact Eclipse for further assistance.

Type:	Blu-ray
Reference:	AACS Specifications
Default Program Action:	Error

Rule ID: 1547

Content Hash Empty

The Content Hash Table is empty.

Background

The CHT contains hashes for each clip file in a BD image. Each hash is calculated on 96 consecutive sectors. This rule indicates that the clip files are less than 96 sectors in length.

Additional Info

When this rule is triggered, the Additional Info column in the Analysis will display one of the following messages.

- Each clip on layer 0 shorter than 96 sectors
- Each clip on layer 1 shorter than 96 sectors

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Warning

Rule ID: 1487

Content ID ISAN

This is an informational rule that reports the International Standard Audiovisual Number (ISAN) when detected on a Blu-ray image. It is required by AACS as a Content Identifier for copy management and online transactions.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Info

Rule ID: 1587

Content owner configuration file

The explanation for this title check rule contains confidential information. Please refer to the studio-specific supplemental rules help PDF document. The document is available from Eclipse Support.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Info

Rule ID: 1716

Content owner configuration file error

The explanation for this title check rule contains confidential information. Please refer to the studio-specific supplemental rules help PDF document. The document is available from Eclipse Support.

Type: Blu-ray
Reference: N/A
Default Program Action: Error

Rule ID: 1717

CPI bits not set in encrypted CPS Unit

An Aligned Unit in an encrypted file was not tagged for encryption.

Background

An Aligned Unit consists of three consecutive sectors of a Clip AV Stream file. When AACS encryption is applied to a Clip AV Stream file (*.m2ts), **all Aligned Units in the file are required to be tagged for encryption**.

Each Clip AV file (*.m2ts) belongs to a Title and each Title belongs to a CPS Unit. For every CPS Unit there is a corresponding CPS Unit Usage File (CPSUnitXXXXX.CCI, where XXXXX = the CPS Unit number to which the CCI file is associated). The CPS Unit Usage File includes information that indicates whether Titles and their Clip AV files under the same CPS Unit are encrypted. On a BDCMF image, Clip AV files that are part of an encrypted CPS Unit must be tagged to indicate that they require to be encrypted. This is done with the Copy Permission Indicator bits in the header of each Aligned Unit.

Severity

It is possible that this error may cause playability problems. Therefore, it is considered an ERROR.

Cause

This problem is caused by the authoring system that created the image.

Solution

This condition is corrected by ImageCopy during the encryption process. If the error occurs on a Type A BD image, then it is not a problem if it will be encrypted with ImageCopy. Note, however, that the EclipseSuite tools will not report this condition on images Type B or later. If ImageCopy is not being used for encryption, you must ensure that the encryption utility you are using can correct this condition. Otherwise, the image must be re-authored.

Type: Blu-ray
Reference: AACS Blu-ray Disc Pre-recorded Book Revision 0.912 Section 7.1
Default Program Action: Error

Rule ID: 1495

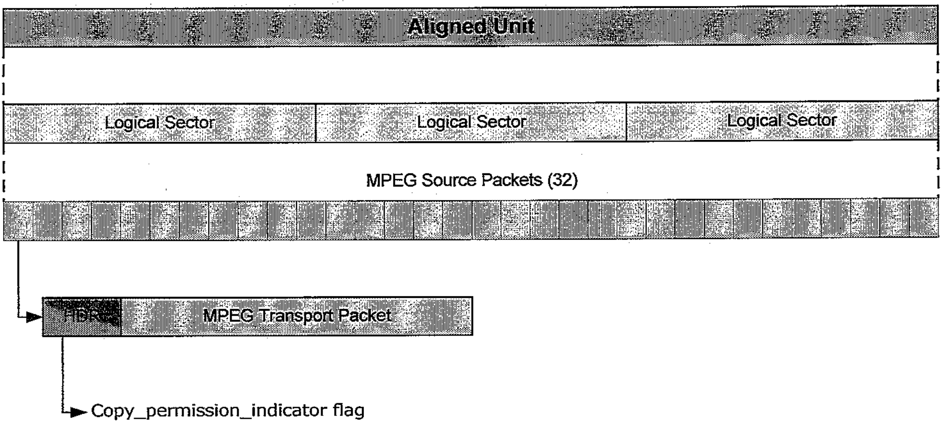
CPI bits set in unencrypted CPS Unit

The copy protection status bits of an Aligned Unit are set indicating that they are encrypted (or need to be encrypted). However, the Aligned Unit is part of a Clip file that belongs to an unencrypted CPS Unit.

Background

Each CPS Unit on a BD image that is encrypted with AACS has an associated CPS Unit Usage file (CPSUnitXXXXX.cci). The CPS Unit Usage file includes bits that specify the protection status of a CPS Unit (e.g. AACS and Macrovision APS). The protection status of a Clip file (*.m2ts) is specified via the Copy Permission Indicator (CPI) bits in the TP_extra_header of the MPEG Source Packets of each Aligned Unit.

Each Clip AV stream file is divided into Aligned Units. An Aligned Unit is equivalent to three logical sectors. Each Aligned Unit is divided into 32 MPEG source packets. An MPEG source packet includes a header where the "Copy_permission_indicator" bits are located. The "Copy_permission_indicator" flag of the first MPEG source packet in the Aligned Unit specifies whether the Aligned Unit is encrypted.



In a BDCMF image, every Clip file is assigned to a CPS Unit. When a Clip file is assigned to an encrypted CPS Unit, the Copy Permission Indicator bits of all the Aligned Units in a Clip file must set to indicate that it requires to be encrypted.

During the analysis of a BD image, the EclipseSuite tools determine the relationship between Clip files and CPS Units. They also determine which CPS Units are encrypted. When analyzing individual Clip AV stream files, the EclipseSuite tools verify that the encryption flags of ALL the Aligned Units in each Clip file match with the encryption status of the CPS Unit that is assigned to the Clip file.

Additional Info

When this rule gets triggered, the **Additional Info** in the Analysis will identify the file where this error got triggered.

'[\STREAM\#####.m2ts]'

This message identifies the Clip file (.m2ts) that contains the Aligned Unit that triggered this error. If this occurs on a source Type A image, this error will be corrected automatically during the conversion to Type B.*

If using older versions of ImageCopy, ImageCopy will only encrypt Aligned Units which have their Copy Protection Indicator bits set. The specifications require that ALL Aligned Units be encrypted if they belong to a Clip file that is assigned to an encrypted CPS Unit. Otherwise, it may result in playability problems.

Similarly, Aligned Units must not be encrypted if they belong to a Clip file that is assigned to a CPS Unit that is not encrypted.

Severity

This rule is set to an ERROR severity since it is known to cause playability problems. However, note that if you are using ImageCopy to encrypt the image then this problem will be automatically corrected. However, this rule will still be triggered during the analysis. If using a version of ImageCopy that corrects this problem, then this rule can be set to a lower severity level.

Cause

This problem is caused by the authoring application that created the image.

Solution

If this problem occurs on a Type A image, then it can be solved if the image is encrypted with ImageCopy. During the encryption process, ImageCopy will override the Copy_permission_indicator bits and ensure that they match with the CPS Unit encryption status.

If this error occurs on a Type B, C, D or disc image, then the image should be re-encrypted using ImageCopy. If not using ImageCopy, the image should be re-authored.

Type:	Blu-ray
Reference:	AACS Specifications
Default Program Action:	Error

Rule ID: 1539

CPS Unit analysis error

An error occurred when the EclipseSuite tools tried to create or read a CPS Unit Key.

Background

During the analysis of a Blu-ray video image, the EclipseSuite tools analyze the CPS Unit Keys. The CPS Unit Keys are stored in the CPS Unit Key File (Unit_Key_RO.inf). On a Type D image and a disc, this file should be encrypted and will be un-encrypted during playback on a Blu-ray player.

During the analysis, the EclipseSuite tools found that the CPS Unit Key File was not encrypted. In order to continue with the analysis, the EclipseSuite tools try to create an in-memory copy of the un-encrypted CPS Unit Key. However, an unexpected error occurs and triggers this rule.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display more details about the failure with one of the following messages.

Severity

This condition is considered a serious problem and, therefore, it is set to an ERROR.

Cause

This problem is caused by the utility that encrypted the image or the encoder that mastered it.

Solution

Contact Eclipse Customer Support for assistance.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

Rule ID: 1574

CPS Unit Key changed at layer break

The CPS Unit Key (a.k.a. Title Key) that is used to encrypt the data changed at the layer transition.

Background

A CPS Unit is a group of Titles to which the same Title Key (CPS Unit Key) has been assigned. Any Clip AV file belonging to the same title is encrypted using the same title key. This error indicates that files belonging to the same Title span between layers. However, the files from the same Title that span into layer 1 appear to have been encrypted with a different Title Key.

Additional Info

When this error occurs, the **Additional Info** column will display more details with the following message.

'[*Filename*]' CPS Unit (*CPSUnitNo*) only valid for layer 0

This message identifies the Title Key (CPS Unit Number) that matches layer 0. The Title Key used on the files on layer 1 for the same Title is invalid.

'[*Filename*]' CPS Unit (*CPSUnitNo*) only valid for layer 1

This message identifies the Title Key (CPS Unit Number) that matches layer 1. The Title Key used on the files on layer 0 for the same Title is invalid.

Severity

This is considered a serious problem since it indicates that files belonging to the same Title are encrypted with different Title Keys. This will likely lead to playability problems. Therefore, it is considered an ERROR.

Cause

This problem is caused by systems that encrypt each layer independently. When this is done, users must ensure that both layers are encrypted with the same keys.

Solution

This condition may be corrected by re-encrypting the original source image using the same Title Key for both layers.

Type:	Blu-ray

Reference: AACS Specifications
Default Program Action: Error

Rule ID: 1554

CPS Unit Key File format error

The Unit Key file is not formatted correctly.

Background

The Unit Key file (Unit_Key_RO.inf) contains the CPS Unit Keys (a.k.a. Title Keys) that were used to encrypt the Clip AV stream files (*.m2ts) in each CPS Unit. The format of this file is as follows:

Unit Key File Syntax

Field	Description
Unit_Key_Block_start_address	Address of Unit_Key_Block within this structure.
Reserved	00h
Unit_Key_File_Header	Header information describing the contents of the Unit Key file.
Padding	00h
Unit_Key_Block	Block containing CPS Unit Keys that are used to encrypt each CPS Unit.
Padding	00h

Unit Key File Header Syntax

Field	Description
Application_Type	= 01h, indicates the type of AV Application which is used with the CPS Unit File. For BDMV Application, this must be set to 1 to indicate that the CPS Unit Key File is associated to the BDMV Application.
Num_of_BD_Directory	= 01h, indicates the number of BD application directories recorded on the media. For BDMV Application, this must be set to 1, because all BDMV applications use only one directory ("\BDMV").
Use_SKB_Unitifed_MKB_Flag	Indicates whether or not Sequence Key Blocks and Unified MKBs are used on the disc.
Reserved	00h
BD Directory List	For each BD Directory (as indicted by Num_of_BD_Directory)...
	CPS_Unit_number for First Playback#I CPS_Unit_number for Top Menu#I Num_of_Titles#I Title List For Each Title J Reserved CPS_Unit_number for Title #J in Directory #I

Unit Key Block Syntax

Field	Description
Number of CPS Units	Indicates the total number of CPS Units on the disc.

Reserved	00h
Unit Key Block List	For each CPS Unit as indicated by Number of CPS Units...
	MAC of PMSNI MAC of DEVICE Binding Nonce Encrypted CPS Unit Key for CPS Unit

Additional Info

When this rule is triggered, the **Additional Info** column will display a more specific message indicating the field that is invalid.

Expecting 'Application_Type' = 1 instead of [*ActualAppType*]

As described in the Unit_Key_Header above, the Application Type of a BD must be set to '1' to indicate that the CPS Unit is associated to the BDMV Application. Any other value is invalid.

Expecting 'Num_of_BD_Directory' = 1 instead of [*ActualNumOfBDDir*]

As described in 'Num_of_BD_Directory' above, this field must be set to 1 to indicate the number of BD Application directories recorded on the media. All Blu-ray video images should include a single '\BDMV' directory.

Sequence Key Blocks/Unified MKBs support not implemented

This condition indicates that the 'Use_SKB_Unified_MKB_Flag' is set, indicating that both Sequence Key Blocks and Unified MKBs are used on the disc. Unfortunately, support for the use of Sequence Key Blocks and Unified MKBs has not been implemented.

'Unit_Key_Block_start_address' ([*Addr*]) is not a multiple of 16 bytes

The Unit Key File is of a fixed structure in which the start of the Unit_Key_Block is always a multiple of 16 bytes. When this condition occurs, it indicates that some fields may not have been included.

Severity

This rule is considered an ERROR since the structure of the Unit Key File is not formatted according to specifications. It is unknown if any of the conditions mentioned above will cause any playability problems.

Cause

This problem is normally caused by the authoring application that created the image.

Solution

The image must be re-authored. Consult with the customer or company that authored the image. Contact Eclipse Support for further assistance.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

Rule ID: 1870

CPS Unit Key File size not a multiple of 65,536 bytes

It is a requirement of the AACS specifications that the size of the CPS Unit Key file (CPS_Unit_RO.inf) be exactly 65,536 bytes.

Background

The AACS specifications define the complete structure of the CPS Unit Key file. Since it is possible that the data contained in this file may not yield a size of 65,536 bytes, the specifications define where padding bytes are added so that the resulting size is 65,536 bytes.

Severity

Although it is unknown if this condition causes any problem, this rule defaults to an ERROR.

Cause

This condition is caused by the authoring application that created the image.

Solution

Consult with the customer or company that authored the image. It is possible that it may need to be re-authored.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

Rule ID: 1869

CPS Unit value not set to zero

The CPS Unit number for a Title, First Playback or Top Menu that doesn't exist is not set to 0.

Background

The Index table file (index.bdmv) includes a list of First Playback, Top Menu and other Titles. When a Title is defined but not recorded, it must be assigned an ID of 0xFFFF.

Similarly, the CPS Unit Key file (Unit_Key_RO.inf) includes a list of First Playback, Top Menu and other Titles. For each Title, it specifies the CPS Unit that the Title is assigned to. If a Title is not recorded, then the CPS Unit number for that Title must be set to 0x0000.

This rule is triggered when the EclipseSuite tools find that the CPS Unit Key file has an entry for a Title that is not recorded and it is assigned a non-zero CPS Unit value.

Additional Info

When this rule is triggered, the Additional Info column in the Analysis will display more details with one of the following messages.

FirstPlayback Title not included in Index Table file

The CPS Unit Key file includes an entry for a First Playback with a non-zero CPS Unit number. However, the First Playback is actually not recorded on the disc. When the First Playback is not recorded, it must assigned a CPS Unit number *value of 0.*

TopMenu Title not included in Index Table file

The CPS Unit Key file includes an entry for a Top Menu with a non-zero CPS Unit number. However, the Top Menu is actually not recorded on the disc. When the Top Menu is not recorded, it must be assigned a CPS Unit number value of 0.

Title ([*Title#*]) not included in Index Table file

A Title entry in the CPS Unit Key file has a non-zero CPS Unit number. However, the Title is actually not recorded on the disc. When a Title is not recorded, then the Title entry in the CPS Unit Key file must be assigned a CPS Unit number value of 0.

Severity

The entry in the CPS Unit Key file for a Title that is not recorded will probably not be referenced by a player. A player will normally access the Titles that are specified in the Index table file. Therefore, this condition is considered a WARNING.

Cause

This condition is caused by the authoring application that created the image.

Solution

The image must be re-authored in order to correct this condition. However, since the Title entry in the CPS Unit Key file that contain the non-zero CPS Unit number will not be accessed by a player, this condition will probably not cause any playability problem. Nevertheless, you should consult with the customer or company that authored the image.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Warning

Rule ID: 1872

CPS Units

This rule report the total number of CPS Units found on a BD image.

Type:	Blu-ray
Reference:	AACS Specifications
Default Program Action:	Info

Rule ID: 1541

Decrypted analog output is prohibited

The image does not support decrypted analog output.

Background

Blu-ray video images can be authored to support Analog and/or Digital output during playback. When this rule is triggered, it indicates that the image has been authored to support Digital Output only. If the end-user's hardware configuration uses the analog output of a Blu-ray player, then this would fail playability.

Digital Only Token

Value	Description
0	Output of decrypted content is allowed for Analog/Digital Outputs.
1	Output of decrypted content is allowed only for Digital Outputs.

The Analog/Digital support is configured in the CPS Unit Usage file (CPSUnitXXXXX.CCI) with the Digital Only Token flag.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will identify the CPS Unit affected by this condition.

CPS Unit ([*CPSUnitNo*])

This message identifies the CPS Unit number that is affected by this condition.

Severity

The severity of this condition depends on whether or not Analog output was intended. If support for both Analog and Digital output was intended, then this condition should be considered an error. However, if Digital output was the only intended option, then this rule should be ignored.

Cause

This problem is caused by the authoring system that created the image.

Solution

If both Analog and Digital were the intended outputs, then this image should be re-authored. If only Digital output was intended, then the image is ok to continue processing.

Type:	Blu-ray
Reference:	AACS Specifications
Default Program Action:	Warning

Rule ID: 1583

Different AACS file

The AACS files used during the encryption process have changed between the source and target images.

This rule is expected to occur when comparing a non-encrypted HDD image to either an AACS-encrypted HDD image or replica.

Background

On an AACS source image, certain encryption files are allocated but the file's data is filled with zeroes.

During the AACS encryption process, the file's data is replaced with the appropriate data. This means that any source before the AACS process compared to an AACS HDD image or title after the AACS process will have this rule activated. It will also be displayed during the verify after copy process during the encryption of the AACS image.

Additional Info Messages

When this rule occurs, the **Additional Info** column in the analysis will display more details about the files that are different. Here are some samples for the additional information:

Blu-ray Sample files

\AACS\MKB_RO.inf
\AACS\MKB_RW.inf
\AACS\ContentRevocation.lst
\AACS\Unit_Key_RO.inf
\AACS\Content000.cer
\AACS\ContentHash000.tbl
Etc.

It will also display the length and location of the files.

Severity

This rule is considered INFO because it is expected that these files are modified during the AACS encryption process and will be different. Our approach is to display the differences in ImageVerify, but in this case only as INFO since they are expected.

Depending on what is being verified, it is good to know if the MKB files used for two different images were the same or not, or if the same title keys were used, or if the Content Certificate was different, or if the Content Revocation List is different, etc. Since ImageVerify displays the differences between two images, we display these as INFO since they are expected.

Type:	Verification
Reference:	AACS Blu-ray Disc Pre-recorded Book, Revision 0.912
Default Program Action:	Flag

Rule ID: 1442

Different amount of Titles

There is a discrepancy between the number of titles listed in the BD Index Table and the number of titles assigned to the CPS Unit Key File.

Background

The BD Index Table is the top-level information for Blu-ray Video. It contains entry points for all Titles, First Play, and Top Menu options. The BD player references the Index Table whenever a Title operation is performed.

The CPS Unit Key File contains all the keys used to encrypt each CPS Unit. A CPS Unit is composed in part by a group of titles, to which a single title key (CPS Unit key) has been assigned for AACS encryption. The CPS Unit Key File contains a "Num_of_Title#" field. This field stores the total number of Titles referenced by the CPS Unit Key File.

Both the CPS Unit Key File and the Index Table must reference all titles in the CPS Unit. If the number of Titles in the CPS Unit Key File is different from the number of Tiles referenced in the Index Table, this warning is triggered.

This warning may also be seen with the error "Clip AV Stream not assigned to a CPS Unit" and the warning "Clip assigned to a CPS Unit", where Eclipse has found an orphaned Clip AV Stream file, but was able to determine to which CPS Unit it should be assigned.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis tab will display more details with the following message.

Index Table ([*No. Titles*]), CPS Unit Key File ([*No. Titles*])

This message shows the difference in number of Titles between the Index Table and CPS Unit Key File.

Error Severity

This rule is currently a warning since there is only one CPS Unit being used at this time. Therefore, it is expected that all Titles be assigned this same CPS Unit. However, in the future, the severity may change when multiple CPS Units are used. If not resolved, this condition can result in an unplayable disc.

Possible Cause

This condition occurs when the image is authored. All Titles must reference a CPS Unit.

Possible Solution

If the image contains only one CPS Unit, as most images do at this time, ImageCopy will assign it to all Titles.

Type:	Blu-ray
Reference:	Blu-ray Read-Only Format & AACS for Prerecorded Specifications
Default Program Action:	Warning

Rule ID: 840

Different Analog Protection System status

The analog copy protection status between the Source and Target differs.

Background

The Analog Protection System (APS) is a form of copy protection that alters the analog signal, which results in poor video and audio quality in illegal copies. This protection system is used in DVD-Video and Blu-ray images.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will indicate the difference with one of the following messages.

source = protected

The Source image is protected with the Analog Protection System but the Target is not.

target = protected

The Target image is protected with the Analog Protection System but the Source is not.

Severity

This rule is considered a WARNING since it indicates a difference in the copy protection status between the Source and Target. It does not indicate a difference in the data. However, you should review the protection status of the Source and Target with the author of the image to find out what was intended.

Cause

It is unknown as to the cause of this condition. However, make sure that you are not comparing two different versions of the same image.

Solution

Contact the author to confirm the APS protection that was intended for this image.

Type:	Blu-ray
Reference:	AACS Specifications
Default Program Action:	Warning

Rule ID: 1545

Different BDCMF and determined M2TS Specific Areas

The BDCMF extent locations for the M2TS Specific Area do not match the actual extent locations found.

Background

The BDCMF file includes extent locations for all Clip files including any 3D SSIF file. In the case of M2TS files, the M2TS Specific Area extents are also identified in the BDCMF. Similarly, the UDF file system of the image includes extents for every file. During analysis, the EclipseSuite will parse the UDF file system of the image and will determine the actual extent locations. This condition occurs when the extent locations specified by the BDCMF do not match the actual extents found during the analysis.

When processing a 3D image, the EclipseSuite tools will use the actual extent information that was found during the analysis.

Severity

It is unknown how this condition may affect playability. Therefore, it is treated as an ERROR.

Cause

This condition is caused by the authoring system that created the image.

Solution

The image must be re-authored.

Type:	3D-BD
Reference:	3D Specifications
Default Program Action:	Error

Rule ID: 1738

Different BDCMF and determined SSIF Specific Areas

The BDCMF extent locations for the SSIF Specific Area do not match the actual extent locations found.

Background

The BDCMF file includes extent locations for all Clip files including any 3D SSIF file. In the case of SSIF files, the SSIF Specific Area extents are also identified in the BDCMF. Similarly, the UDF file system of the image includes extents for every file. During analysis, the EclipseSuite will parse the UDF file system of the image and will determine the actual extent locations. This condition occurs when the extent locations specified by the BDCMF do not match the actual extents found during the analysis.

When processing a 3D image, the EclipseSuite tools will use the actual extent information that was found during the analysis.

Severity

It is unknown how this condition may affect playability. Therefore, it is treated as an ERROR.

Cause

This condition is caused by the authoring system that created the image.

Solution

The image must be re-authored.

Type:	3D-BD
Reference:	3D Specifications
Default Program Action:	Error

Rule ID: 1737

Different BDCMF and estimated HDMV Region playback

The region code specified in BDCMF is different from the one found during the region code analysis.

Background

Determining and reporting the region code settings on a Blu-ray title is not a simple task. The region code instructions are embedded deep into the content and cannot be determined without sophisticated analysis. To address this, the Region Coding of a disc can also be summarized in the BDCMF. Unfortunately, the region code information in the BDCMF is not always complete or accurate. EclipseSuite attempts to nalyze, validate, and report the BDCMF and HDMV region code data. Region code analysis is not upported for BD+ and BD-J titles.

The region coding method of Blu-ray is more sophisticated than the DVD implementation. With DVD, the ntire disc was assigned a region code. All titles on a disc were assigned the same region code which could asily be read from the Control Data and Video Manager file. With Blu-ray, however, it is possible to set egion codes for each individual title on the disc. The region code instructions are contained in the avigational PlayLists of the title. This region code implementation gives authors flexibility when letermining how a disc will behave in players from each region. As a result, the EclipseSuite tools must arse through the navigational commands to determine in which regions each title is allowed to play. 3lu-ray region coding divides the world into regions A, B, and C. Each region can have one of the ollowing attributes:

llowed - The entire disc can be played back.
imited - Only a part of the disc can be played back.
rohibited - The entire disc can't be played back.
Not Applicable - The authoring studio cannot set Region.

3DCMF Images

f completed by the authoring software, EclipseSuite will report the region codes found in the BDCMF mage "Region Code" element by displaying it on the analysis tab of the EclipseSuite application. It is mportant to note that the region code flags in the BDCMF do not provide instructions to the encoder or ncryption engine and do not directly control the region code instructions in the actual image. They are here for reference only and, therefore, do not provide a definitive depiction of the actual region coding on he disc. Ideally, the BDCMF image will always include the region code information and it will always be ccurate.

3lu-ray movies are authored using one of two authoring formats. HDMV Content is the basic method of uthoring titles. BD-Java is a more advanced authoring style that can take full advantage of the BD-Java rogramming layer.

HDMV Content

When analyzing replicas and BDCMF images, EclipseSuite will parse the HDMV content to determine the egion code data. This information will be displayed on the Video Attributes page in the Info tab. Each egion will list the clips and titles assigned to that region code.

3D-Java Content

Region coding can also be managed through the BD-J programming language. At this time, EclipseSuite annot determine the region code of BD-J titles. For BD+ images, it is likely that the BD+ security layer will revent an accurate determination of the region code.

Additional Info

When this rule is triggered, the **Additional Info** column in the analysis will display the differences with one of the following messages.

Region A in BDCMF (*BDCMFRegionASetting*), HDMV judgment (*HDMVRegionASetting*)

This message shows the difference between Region A setting specified in the BDCMF.CMF file vs. the one found by the EclipseSuite tools during the analysis.

Region B in BDCMF (*BDCMFRegionBSetting*), HDMV judgment (*HDMVRegionBSetting*)

This message shows the difference between Region B setting specified in the BDCMF.CMF file vs. the one found by the EclipseSuite tools during the analysis.

Region C in BDCMF (*BDCMFRegionCSetting*), HDMV judgment (*HDMVRegionCSetting*)

This message shows the difference between Region A setting specified in the BDCMF.CMF file vs. the one found by the EclipseSuite tools during the analysis.

Severity

The region specified in the BDCMF is used for informational purposes and may not always be accurate. Therefore, it does not provide a definitive depiction of the actual region coding on the disc. For this reason, this rule is considered a WARNING only.

Cause

This condition is caused by the authoring system that created the image.

Solution

This rule does not necessarily indicate a problem with the image. The region code reported in the Video Attributes is more accurate than the ones in reported in the analysis. You can confirm with the authors that the region codes reported in the Video Attributes are the ones that were intended.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Warning

Rule ID: 1782

Different BDCMF subfolder file count

The explanation for this title check rule contains confidential information. Please refer to the studio-specific supplemental rules help PDF document. The document is available from Eclipse Support.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

Rule ID: 1745

Different PIC Field

The Push/Pull Polarity Flags in the PIC data are different.

Background

The Push/Pull Polarity Flag in the PIC data indicates the recording method of a layer as In-Pit recording (negative) or On-Pit recording (positive). The Push/Pull Polarity Flags also indicate how a layer is molded. The setting for the Push/Pull Polarity Flags that are used in mastering are not determined until mastering time. However, since the PIC.DAT file must be supplied by the authoring facility, the flags are set to either

In-Pit or On-Pit. During mastering, the LBR can override the setting.

This rule is triggered when comparing two images and the Push/Pull Polarity flags are different between the two. However, it is more common when comparing a replicated disc to the original source image, indicating that the LBR has overridden the original source image Push/Pull Polarity Flag value.

Additional Info

When this rule is triggered, the **Additional Info** column will display the setting of the Push/Pull Polarity Flags of the source and target images.

Layer [*LayerNo*] Push/Pull Polarity Flags, Source ([*SourceValue*]), Target (*TargetValue*)

This message identifies the layer number and the Push/Pull Polarity Flag values for the Source and Target images. Note that this message does not indicate an error since is normal for these values to be changed during mastering. However, be aware that different polarity values require different molding methods.

Severity

This rule does not indicate a problem with the image since is normal for these values to be changed during mastering. However, be aware that different polarity values require different molding methods.

Cause

When the image is authored, the authoring system will set the polarity flag to either negative or positive. However, replicators can choose from either recording method (In-Pit or On-Pit) during mastering.

Solution

This rule does not indicate a problem with the image. It is only an informational message that identifies the recording method of two images.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Flag

Rule ID: 1567

Different Volume ID

The Volume ID of the Source is not the same as the Volume ID of the Target

Background

The Volume ID (VID) is a component of the Blu-ray encryption system and is used to encrypt the title key files of a BD image. The VID is generated by the Eclipse encoder during mastering and is linked to the ROM-Mark Inserter of the LBR. The VID is then written to the BDCMF file.

Each time the image is subsequently mastered, the Eclipse encoder checks the VID in the CMF to see if it matches the RMI unit. If the VID is valid for that RMI unit, then the VID in the CMF is used. If not, as in the case of cutting on a different LBR with a different RMI, the Eclipse encoder will generate a new VID.

Generating a new Volume ID is not a problem as long as the VID is valid and is properly applied to the title keys.

Severity

This rule is set to Flag only as Different Volume ID is expected certain production environments.

Cause

Because the Volume ID is linked to a particular ROM-Mark Inserter unit, the Volume ID will be change if the title is mastered on different LBR's.

Solution

The Different Volume ID rule by itself is not a problem.

The important thing is that Volume ID is valid and that the title keys can be decrypted properly. If the Volume ID is invalid, the Eclipse analysis engine will fail to decrypt the content and will report other serious errors, including comparison errors.

Type:	Blu-ray
Reference:	BDCMF Specifications
Default Program Action:	Flag

Rule ID: 1559

Directory not in Authoring Studio namespace

The explanation for this title check rule contains confidential information. Please refer to the studio-specific supplemental rules help PDF document. The document is available from Eclipse Support.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

Rule ID: 1821

Disc PAC content error

An error occurred when trying to read the PAC data from the disc.

Background

During analysis of a Blu-ray disc, the EclipseSuite tools attempt to read the PAC data. This rule indicates that the drive failed to read this information. This may indicate a physical defect on the media or an incompatibility of the drive.

Currently, the PAC information is not used. Therefore, if the media is being used as a source disc for mastering, then this condition is not considered serious since ImageCopy will automatically generate the PAC information on the output image. If the disc is a replica, verify that there are no physical defects.

Severity

This condition normally occurs on Blu-ray recordable media. Since the PAC information is currently not used and ImageCopy can re-generate it during loading, this condition is only considered a WARNING.

Cause

This condition normally occurs when the drive is unable to read the PAC data assumed because of physical defects.

Solution

If this occurs on a disc that is being used as a master, then this condition can be ignored since ImageCopy can re-generate the PAC data.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Warning

Rule ID: 1826

Disc version is newer than Title Structure configuration

The disc version in the Disc Properties file is newer than expected.

Background

EclipseSuite 4.0 Beta N (June 2011) implemented a new version of the Title Structure Analysis for Fox & MGM studios. This rule indicates that the image being analyzed meets most of the pre-requisites so that the new Title Structure analysis can be performed. However, the disc version has a value that is newer than what was expected. The EclipseSuite tools will apply the current Title Structure Analysis they support. However, the newer disc version might indicate that there is a newer version of the Title Structure specifications and you are using an older version of the EclipseSuite tools that does not support it. It can also indicate that authoring specified the wrong version.

Severity

This condition is considered a WARNING since the EclipseSuite tools are expecting a different value for the disc version.

Cause

Confirm that you are using the latest version of the EclipseSuite tools that support the most current version of Fox's Title Structure specifications. If you are using the correct version of EclipseSuite, then it may indicate that authoring specified the wrong disc version.

Solution

Confirm that you are using the latest version of the EclipseSuite tools that supports the most current version of Fox's Title Structure specifications. If you are using the correct version of EclipseSuite, then consult with Fox Studios to see if this condition is acceptable to continue or whether the image should be re-authored.

Type:	Blu-ray

Reference: N/A
Default Program Action: Warning

Rule ID: 1860

Elementary HDMV stream not found

A stream is missing from a PlayItem.

Background

A PlayItem includes fields which specify the number of:

- Primary video streams
- Primary audio streams
- Presentation Graphics / Text subtitle stream
- Interactive Graphics stream
- Secondary audio stream
- Secondary video stream

All of the streams are described in another area of the PlayItem. This rule is triggered when the actual number of each of the above streams does not match the number that was originally specified.

Additional Info

When this rule is triggered, the **Additional Info** column in the analysis will identify the stream that is missing with one of the following messages.

Primary video stream id ([*VID*]), PID [*StreamTypeID*], PlayList '[*PlayListFileName*]', clip AV stream file '[*ClipAVStreamFilename*]'

This message indicates that a PlayItem specified a number of Primary Video Streams but when the EclipseSuite tools searched for all, the one specified by VID was not found.

Primary audio stream id ([*VID*]), PID [*StreamTypeID*], PlayList '[*PlayListFileName*]', clip AV stream file '[*ClipAVStreamFilename*]'

This message indicates that a PlayItem specified a number of Primary Audio Streams but when the EclipseSuite tools searched for all, the one specified by VID was not found.

PG text subtitle stream id ([*VID*]), PID [*StreamTypeID*], PlayList '[*PlayListFileName*]', clip AV stream file '[*ClipAVStreamFilename*]'

This message indicates that a PlayItem specified a number of Presentation Graphics & Text Subcode Streams but when the EclipseSuite tools searched for all, the one specified by VID was not found.

IG stream id ([*VID*]), PID [*StreamTypeID*], PlayList '[*PlayListFileName*]', clip AV stream file '[*ClipAVStreamFilename*]'

This message indicates that a PlayItem specified a number of Interactive Graphics Streams but when the EclipseSuite tools searched for all, the one specified by VID was not found.

Secondary audio stream id ([*VID*]), PID [*StreamTypeID*], PlayList '[*PlayListFileName*]', clip AV stream file '[*ClipAVStreamFilename*]'

This message indicates that a PlayItem specified a number of Secondary Audio Streams but when the EclipseSuite tools searched for all, the one specified by VID was not found.

Secondary video stream id ([*VID*]), PID [*StreamTypeID*], PlayList '[*PlayListFileName*]', clip AV stream file '[*ClipAVStreamFilename*]'

This message indicates that a PlayItem specified a number of Secondary Video Streams but when the EclipseSuite tools searched for all, the one specified by VID was not found.

Severity

It is unknown if this condition will cause any playability problems. Therefore, it is considered a WARNING.

Cause

This problem is typically caused by the authoring application that created the image.

Solution

The image must be re-authored.

Type:	Blu-ray
Reference:	Blu-ray Video Specifications
Default Program Action:	Warning

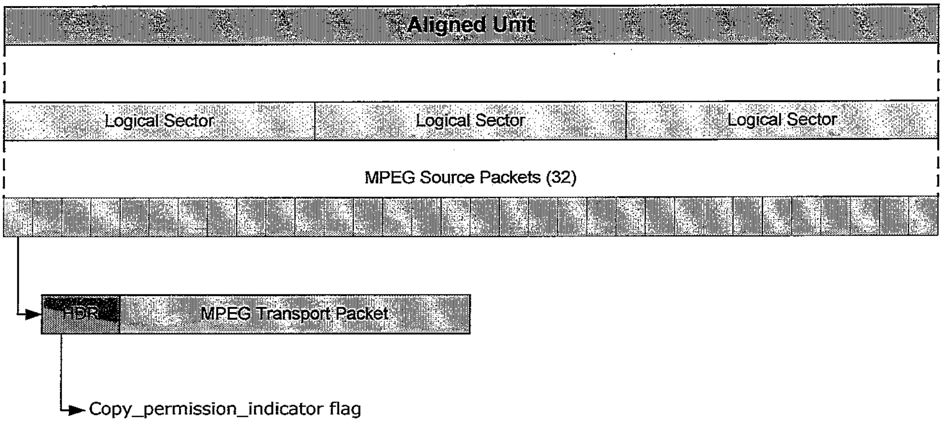
Rule ID: 1656

Encrypted aligned unit does not have CPI bits set

An Aligned Unit belongs to an encrypted Clip file that is assigned to an encrypted CPS Unit. However, the Aligned Unit's CPI bits indicate that it is not encrypted.

Background

Clip files consist of Aligned Units. Each Clip file is assigned to a CPS Unit which may or may not be encrypted. When a Clip file is assigned to an encrypted CPS Unit, the **Copy Permission Indicator** (CPI) bits in ALL of the Aligned Units in the Clip must be set to indicate that they are (or will be) encrypted. This condition can be corrected by ImageCopy during the encryption process.



Severity

The specifications require that if a Clip is assigned to an encrypted CPS Unit then all the Aligned Units in the Clip must be encrypted. If not all Aligned Units are encrypted, then it may lead to playability problems. It is for this reason that this is considered an ERROR. Note, however, that ImageCopy is able to correct this condition.

Cause

This condition is caused by the authoring application that created the image.

Solution

If you are using ImageCopy, this problem can be corrected when the image is encrypted (i.e. conversion from Type A to Type B). Although this error is still reported, the output image will no longer have the error.

If you are not using ImageCopy and the utility that encrypts the image does not correct this condition, then the image may need to be re-authored.

Type:	Blu-ray
Reference:	AACS Specifications
Default Program Action:	Error

Rule ID: 1570

Encrypted aligned unit in unencrypted CPS Unit

The protection status of an Aligned Unit does not match with the protection status of the CPS Unit that it is assigned to.

Background

Clip files consist of an integer number of Aligned Units. Each Aligned Unit consists of 3 logical sectors. Each Aligned Unit includes the Copy Protection Indicator bits that indicate whether the Aligned Unit is encrypted. If a Clip file is assigned to an encrypted CPS Unit, then the CPI bits of ALL the Aligned Units in the Clip must be set to indicate that they are (or will be) encrypted. Similarly, if a Clip file is assigned to an un-encrypted CPS Unit, then the CPI bits of ALL the Aligned Units must be set to indicate that they are not (or don't need to be) encrypted.

Severity

If the CPI bits of an Aligned Unit do not match the protection status of the CPS Unit that its parent Clip file, then it may cause playability problems. Therefore, this condition is considered an ERROR.

Cause

This problem is caused by the authoring application that created the image.

Solution

If you are using ImageCopy, then this condition will be corrected automatically when the image is encrypted (i.e. conversion from Type A to Type B). Although this error is still triggered during the encryption process, the output image will no longer have this error.

If you are not using ImageCopy and the utility you are using to encrypt the image does not correct the problem, then the image must be re-authored.

Type:	Blu-ray
Reference:	AACS Specifications
Default Program Action:	Error

Rule ID: 1572

Enhanced Title

This is an informational rule that identifies an Enhanced Title. An Enhanced Title is Title that requires permission from a remote server before playback. Therefore, this implies that the image must also include at least one BD-Java application that will connect to the remote server.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Info

Rule ID: 1862

Enhanced Title requires BD-J Application

The Blu-ray image includes a Title that has been identified as an Enhanced Title but the image does not include a BD-J application.

Background

An Enhanced Title is Title that requires permission from a remote server before playback. Therefore, this implies that the image must also include at least one BD-Java application that will connect to the remote server. This rule indicates that an Enhanced Title is present but no BD-Java applications were found.

Severity

This rule is considered an ERROR since it is known to cause playability problems.

Cause

This condition is caused during authoring of the image.

Solution

The image must be re-authored.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

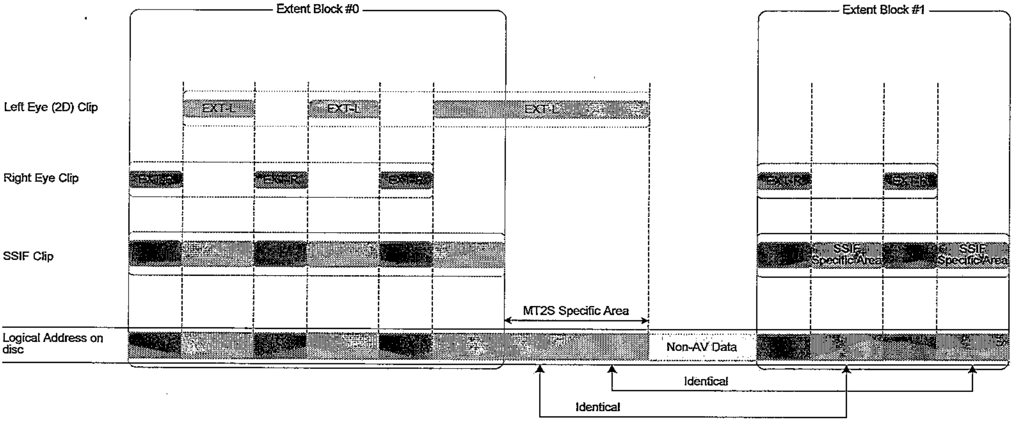
Rule ID: 1863

Equivalent 2D data block not found

The M2TS file does not include an extent that is present in the SSIF AV Stream file.

Background

The SSIF file is constructed from extents from the left and right eye AV Stream files (except for the M2TS Specific Areas). Every extent in the 2D (left eye) M2TS file, except the M2TS Specific Area, must be included in the SSIF file. This condition indicates that an extent exists in the SSIF file but not in the 2D Clip file.


Extent Block #0
Extent Block #1
Left Eye (2D) Clip
Right Eye Clip
SSIF Clip
Logical Address on disc
EXT-L
EXT-L
EXT-L
EXT-R
EXT-R
EXT-R
EXT-R
EXT-R
SSIF Specific Area
SSIF Specific Area
MT2S Specific Area
Non-AV Data
Identical
Identical

Additional Info

When this condition occurs, the **Additional Info** column in the Analysis will identify the extent, 2D M2TS and SSIF files.

Found left view data block B[*ExtNo*] for '[*SSIF_File*]', but not for '[*M2TS_File*]'

This message identifies the extent that is found in the SSIF file but not in the M2TS file.

Severity

It is unknown how this may affect playability. Therefore, it is treated as an ERROR.

Cause

This condition is caused by the authoring system that created the image.

Solution

The image must be re-authored. Contact Eclipse Customer Support for further assistance.

Type:	3D-BD
Reference:	N/A
Default Program Action:	Info

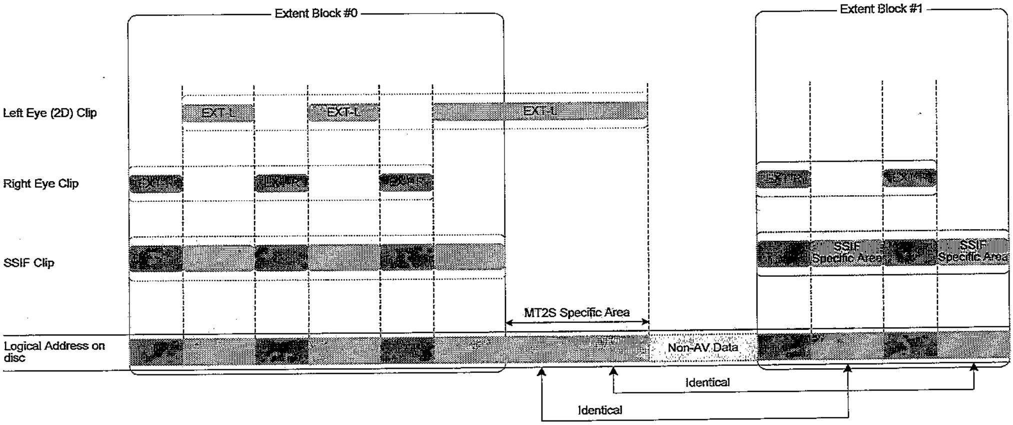
Rule ID: 1756

Equivalent Base data block not found

The SSIF file does not include an extent that is present in the 2D M2TS AV Stream file or the extents are different.

Background

The SSIF file is constructed from extents from the left and right eye AV Stream files (except for the M2TS Specific Areas). Every extent in the 2D (left eye) M2TS file, except the M2TS Specific Area, must be included in the SSIF file. This condition indicates that an extent exists in the 2D Clip file but not in the SSIF file. Or, the extent exists in both files but one extent is longer than the other.


Extent Block #0
Extent Block #1
Left Eye (2D) Clip
Right Eye Clip
SSIF Clip
Logical Address on disc
EXT-L
EXT-L
EXT-L
SSIF Specific Area
SSIF Specific Area
MT2S Specific Area
Non-AV Data
Identical
Identical

Additional Info

When this condition occurs, the **Additional Info** column in the Analysis will identify the extent, 2D M2TS and SSIF files.

Found 2D data block B[*ExtNo*] for '[*M2TS_File*]', but not for '[*SSIF_File*]'

This message indicates that the extent B[#], was found in the M2TS Clip file but not in the SSIF file.

Data block B[*ExtNo*] for '[*M2TS_File*]' has length ([*Length*]) but for '[*SSIF_File*]' it has ([*Length*])

This message indicates that both M2TS and SSIF include the extent but the extent length is different between the two files.

Severity

It is unknown how this may affect playability. Therefore, it is treated as an ERROR.

Cause

This condition is caused by the authoring system that created the image.

Solution

The image must be re-authored. Contact Eclipse Customer Support for further assistance.

Type:	3D-BD
Reference:	3D Specifications
Default Program Action:	Error

Rule ID: 1755

Equivalent M2TS Specific Area not found

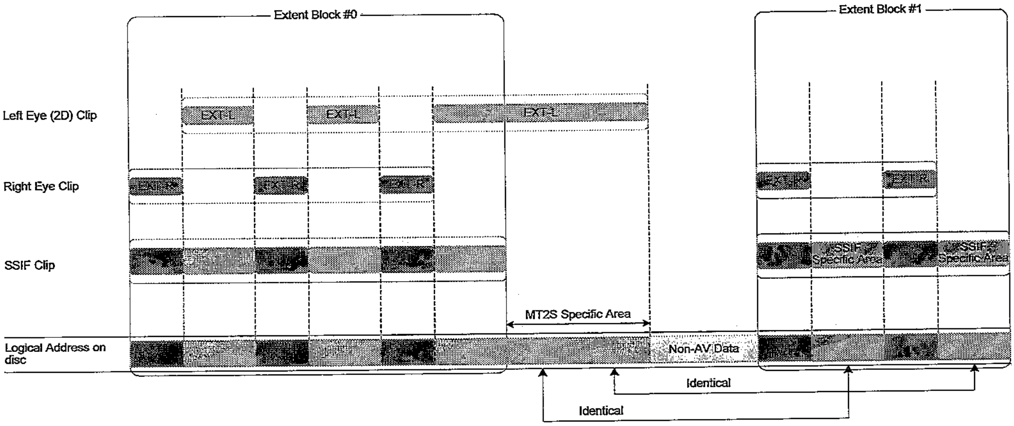
An SSIF Specific Area exists without a matching M2TS Specific Area.

Background

Each SSIF file is associated with two M2TS files. One of these M2TS files includes the normal A/V data for 2D playback (2D Clip). From this file, most of the A/V data is used for the left eye view for 3D playback. The part of the 2D Clip that is not included in the left eye Clip is called the 'M2TS Specific Area'. This data is duplicated and recorded in the SSIF file in the area called 'SSIF Specific Area' (i.e. data in M2TS Specific Area = data in SSIF Specific Area). The other M2TS file includes the A/V data for the right eye view for 3D playback. The SSIF file consists of all the A/V data from the left and right eye files.

This error indicates that an M2TS Specific Area was detected but no matching SSIF Specific Area in the associated SSIF file.

The following picture shows an example of the file extents in a 3D image.


Extent Block #0
Extent Block #1
Left Eye (2D) Clip
EXT-L
EXT-L
EXT-L
Right Eye Clip
EXT-R
EXT-R
EXT-R
EXT-R
EXT-R
SSIF Clip
SSIF Specific Area
SSIF Specific Area
MT2S Specific Area
Logical Address on disc
Non-AV Data
Identical
Identical

Severity

It is unknown how this may affect playability. Therefore, it is treated as an ERROR.

Cause

This condition is caused by the authoring system that created the image.

Solution

The image must be re-authored. However, since the writing of this topic, the 3D Specifications were not finalized. Check with the author of the image to confirm the severity of this condition.

Type:	3D-BD
Reference:	3D Specifications
Default Program Action:	Error

Rule ID: 1740

Equivalent SSIF Specific Area not found

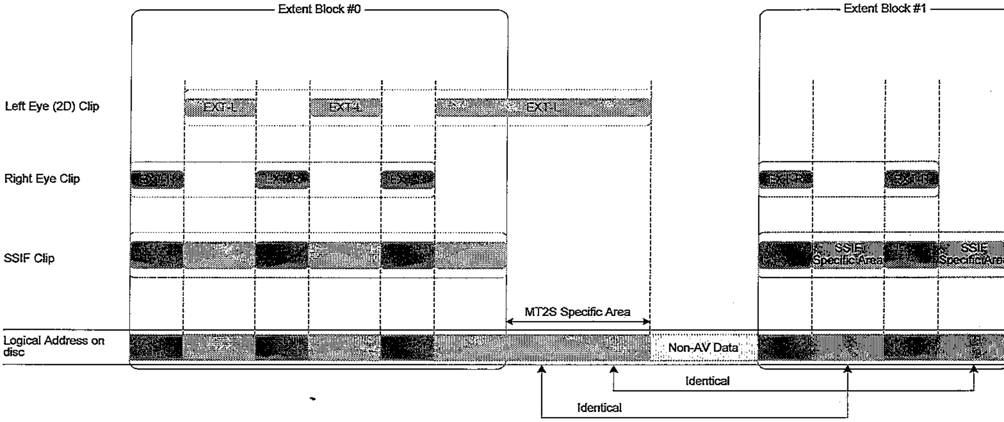
An M2TS Specific Area exists without a matching SSIF Specific Area.

Background

Each SSIF file is associated with two M2TS files. One of these M2TS files includes the normal A/V data for 2D playback (2D Clip). From this file, most of the A/V data is used for the left eye view for 3D playback. The part of the 2D Clip that is not included in the left eye Clip is called the 'M2TS Specific Area'. This data is duplicated and recorded in the SSIF file in the area called 'SSIF Specific Area' (i.e. data in M2TS Specific Area = data in SSIF Specific Area). The other M2TS file includes the A/V data for the right eye view for 3D playback. The SSIF file consists of all the A/V data from the left and right eye files.

This error indicates that an M2TS Specific Area was detected but no matching SSIF Specific Area in the associated SSIF file.

The following picture shows an example of the file extents in a 3D image.


Extent Block #0
Extent Block #1
Left Eye (2D) Clip
Right Eye Clip
SSIF Clip
Logical Address on disc
EXT-L
EXT-L
EXT-L
EXT-R
EXT-R
EXT-R
EXT-R
EXT-R
SSIF Specific Area
SSIF Specific Area
MT2S Specific Area
Non-AV Data
Identical
Identical

Severity

It is unknown how this may affect playability. Therefore, it is treated as an ERROR.

Cause

This condition is caused by the authoring system that created the image.

Solution

The image must be re-authored. However, since the writing of this topic, the 3D Specifications were not finalized. Check with the author of the image to confirm the severity of this condition.

Type:	3D-BD
Reference:	3D Specifications
Default Program Action:	Error

Rule ID: 1739

Estimated HDMV Region playback

This is an informational rule that identifies the 'possible' regions that the Blu-ray Video is compatible with.

Background

Determining and reporting the region code settings on a Blu-ray title is not a simple task. The region code instructions are embedded deep into the content and cannot be determined without sophisticated analysis. To address this, the Region Coding of a disc can also be summarized in the BDCMF. Unfortunately, the region code information in the BDCMF is not always complete or accurate. EclipseSuite attempts to analyze, validate, and report the BDCMF and HDMV region code data. Region code analysis is not supported for BD+ and BD-J titles.

The region coding method of Blu-ray is more sophisticated than the DVD implementation. With DVD, the ntire disc was assigned a region code. All titles on a disc were assigned the same region code which could asily be read from the Control Data and Video Manager file. With Blu-ray, however, it is possible to set egion codes for each individual title on the disc. The region code instructions are contained in the avigational PlayLists of the title. This region code implementation gives authors flexibility when etermining how a disc will behave in players from each region. As a result, the EclipseSuite tools must arse through the navigational commands to determine in which regions each title is allowed to play.

lu-ray region coding divides the world into regions A, B, and C. Each region can have one of the following ttributes:

llowed - The entire disc can be played back.
imited - Only a part of the disc can be played back.
rohibited - The entire disc can't be played back.
ot Applicable - The authoring studio cannot set Region.

DCMF Images

f completed by the authoring software, EclipseSuite will report the region codes found in the BDCMF mage "Region Code" element by displaying it on the analysis tab of the EclipseSuite application. It is mportant to note that the region code flags in the BDCMF do not provide instructions to the encoder or ncryption engine and do not directly control the region code instructions in the actual image. They are here for reference only and, therefore, do not provide a definitive depiction of the actual region coding on he disc. Ideally, the BDCMF image will always include the region code information and it will always be ccurate.

lu-ray movies are authored using one of two authoring formats. HDMV Content is the basic method of uthoring titles. BD-Java is a more advanced authoring style that can take full advantage of the BD-Java rogramming layer.

DMV Content

Vhen analyzing replicas and BDCMF images, EclipseSuite will parse the HDMV content to determine the egion code data. This information will be displayed on the Video Attributes page in the Info tab. Each egion will list the clips and titles assigned to that region code.

D-Java Content

egion coding can also be managed through the BD-J programming language. At this time, EclipseSuite annot determine the region code of BD-J titles. For BD+ images, it is likely that the BD+ security layer will revent an accurate determination of the region code.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Info

ule ID: 1781

xtent of file is less than 500,000 bytes

ll file extents for the 3D files must have a size greater than or equal to 500,000 bytes, except the last extent f the files.

Background

The Blu-ray specifications for 3D require all extents of the 3D files to be greater than or equal to 500,000 bytes.

Severity

It is unknown how this may affect playability. However, the specifications clearly describe a set of rules to be followed for the 3D files. One of these rules is the required minimum size of the file extents. This rule defaults to an ERROR condition.

Cause

This condition is caused by the authoring system that created the image.

Solution

The image must be re-authored. Contact Eclipse Support for further assistance.

Type:	Blu-ray
Reference:	Blu-ray Disc Read-Only Format Part 3: Audio Visual Basic Specifications (3-1 Core Specifications) Annex P Main requirements for Stereoscopic 3D
Default Program Action:	Error

Rule ID: 1784

Extent size not on AU boundary

The extent length of a Clip file does not end with an Aligned Unit.

Background

A Clip AV file (*.m2ts) consists of an integer number of Aligned Units, where each Aligned Unit consists of 3 logical sectors. In UDF, the allocation of a Clip AV file is described with one or more Extents. An Extent describes the location and length of the file's data. Since an Extent can only describe up to 1GB, then more than one Extent are required for larger files. The AACS Specifications require that each Extent length be an integer number of Aligned Units. This means that the last sector of an Extent must also be the last sector of an Aligned Unit.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will identify the Clip file and the start address and length of the Extent that triggered this rule.

File [#####*.m2ts*], Extent starting at [*ExtentStartAddr*], length [*Length*]

This message identifies the Clip file (.m2ts) and the start address and length of the Extent that triggered this rule. The length is expressed in number of logical sectors. The AACS specifications require that the Extent end with an Aligned Unit.*

Severity

It is unknown if this condition will cause any playability problems. However, it is a violation of the AACS specifications. Therefore, it is considered an ERROR.

Cause

This problem is caused by the authoring system that created this image.

Solution

This problem cannot be corrected in the pre-mastering or mastering process. The image must be re-authored.

Type:	Blu-ray
Reference:	AACS Specifications Annex A
Default Program Action:	Error

Rule ID: 1584

Extent size too big for 3D Output Mode

The extent size of a 3D file extent has exceeded the maximum allowed by the specifications.

Background

The Blu-ray 3D specifications define several rules that must be followed. One of these limits de size of extents based on several conditions.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will identify the extent, the maximum size allowed and the actual size.

Severity

It is unknown how this condition may affect playability. However, the specifications clearly define these rules. Therefore, this condition defaults to an ERROR.

Cause

This condition is caused by the authoring system that created the image.

Solution

The image must be re-authored. Contact Eclipse Support for further assistance.

Type:	Blu-ray
Reference:	Blu-ray Disc Read-Only Format Part 3: Audio Visual Basic Specifications (3-1 Core Specifications) Annex P Main requirements for Stereoscopic 3D
Default Program Action:	Info

Rule ID: 1786

Extent size too small for 2D Output Mode

One of the extents in a Clip AV file of a 3D image is too small for 2D Output Mode.

Background

A 3D Blu-ray image can be played in the traditional 2D mode (2D Output Mode) or 3D (3D Output Mode). In order to guarantee seamless playback in either mode, the specifications require a minimum size for the extents that make up the Clip AV files. This condition indicates that the EclipseSuite tools detected an extent smaller than what the specifications require.

Severity

It is unknown how this may affect playability. Therefore, it is considered an ERROR.

Cause

This condition is caused by the authoring system that created the image.

Solution

The image must be re-authored. Contact Eclipse Support for further assistance.

Type:	3D
Reference:	Blu-ray Specifications Annex 9: Main requirements for Stereoscopic 3D
Default Program Action:	Error

Rule ID: 1767

Extent size too small for 3D Output Mode

One of the extents in a Clip AV file of a 3D image is too small for 3D Output Mode.

Background

A 3D Blu-ray image can be played in the traditional 2D mode (2D Output Mode) or 3D (3D Output Mode). In order to guarantee seamless playback in either mode, the specifications require a minimum size for the extents that make up the Clip AV files. This condition indicates that the EclipseSuite tools detected an extent smaller than what the specifications require.

Severity

It is unknown how this may affect playability. Therefore, it is considered an ERROR.

Cause

This condition is caused by the authoring system that created the image.

Solution

The image must be re-authored. Contact Eclipse Support for further assistance.

Type:	3D
Reference:	Blu-ray Specifications Annex P: Main requirements for Stereoscopic 3D
Default Program Action:	Error

Rule ID: 1768

Failed to load file

The EclipseSuite programs were unable to load a file for processing.

Background

Part of the BD-Java security analysis is to validate the files that are used for online connectivity. The files are as follows:

app.discroot.crt
online.sig
online.crl
online.crt

When this rule is triggered, it indicates that the EclipseSuite tools were unable to find one of these files.

Severity

This rule is considered an ERROR since these files are required when users connect to an online server.

Cause

If the files are not included, then it is an authoring problem.

Solution

Consult with the author of the image to see if these files were intended to be included with the image. The image may need to be re-authored. Check with Eclipse Customer Support for further assistance.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

Rule ID: 1661

File Allocated on the wrong layer

A Content Certificate file or Content Hash Table file that is supposed to be recorded on layer 1 has been detected on layer 0.

Background

The AACS specifications define Content Certificate and Content Hash Table files. These files contain AACS encryption information specific to the files recorded on each layer. The files are as follows:

Filename	Description
\AACS\CONTENT000.CER	Layer 0 Content Certificate File
\AACS\CONTENT001.CER	Layer 1 Content Certificate File
\AACS\CONTENTHASH000.TBL	Layer 0 Content Hash Table File
\AACS\CONTENTHASH001.TBL	Layer 1 Content Hash Table File

\AACS\DUPLICATE\CONTENT000.CER \AACS\DUPLICATE\CONTENT001.CER \AACS\DUPLICATE\CONTENTHASH000.TBL \AACS\DUPLICATE\CONTENTHASH001.TBL	Duplicate copy of the files above

Additional Info

When this rule is triggered, the **Additional Info** column in the analysis will identify the file with one of the following messages.

ContentHash001.TBL expected on layer 1

This message identifies the file CONTENTHASH001.TBL as being allocated on layer 0 instead of layer 1 as required by the specifications.

\Duplicate\ContentHash001.TBL expected on layer 1

This message identifies the file \DUPLICATE\CONTENTHASH001.TBL as been allocated on layer 0 rather than layer 1 as required by the specifications.

Content001.CER expected on layer 1

This message identifies the file CONTENT001.CER as being allocated on layer 0 rather than layer 1 as required by the specifications.

\Duplicate\Content001.CER expected on layer 1

This message identifies the file \DUPLICATE\CONTENT001.CER as being allocated on layer 0 rather than layer 1 as required by the specifications.

Error Severity

Although this condition is not known to cause any playability problems, it is still not to specifications and, therefore, is considered an error.

Possible Cause

This problem is caused when the image is authored.

Possible Solution

This image must be re-authored.

Type:	Blu-ray
Reference:	AACS Blu-ray Disc Pre-recorded Book Revision 0.912 2.1 & 2.3
Default Program Action:	Error

Rule ID: 1445

File comparison error

An error occurred while comparing two files.

Background

Some formats such as Blu-ray have copies of files as backups. During the analysis, the EclipseSuite tools will compare the original file to the backup and report any errors. This rule is triggered if the files are not the same, if one is missing, if one can't be loaded for comparison, etc.

Additional Info

When this rule is triggered, the **Additional Info** column in the analysis will identify the file and provide more details.

Severity

This rule indicates possible file corruption. Therefore, it is considered an ERROR.

Cause

There are many conditions that may cause this rule to be triggered. Some may be due to authoring problems.

Solution

Contact Eclipse Customer Support.

Type:	UDF
Reference:	N/A
Default Program Action:	Error

Rule ID: 866

File extents not allocated with ascending order

The extents belonging to a file were not recorded in ascending order as required by the specifications.

Background

The Blu-ray specifications allow files to be recorded in multiple extents. However, the specifications require that the extents be recorded in ascending order.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will identify the file in question.

Severity

This requirement is typically due to performance reasons. When extents are recorded in random order, a playback device must perform more seek operations in order to read the file data. This has a direct effect on performance and may cause playability problems if it occurs on a video file. It is for this reason that this error is considered an ERROR.

Cause

This error is caused by the authoring system that created the image.

Solution

The image must be re-authored.

Type:	UDF
Reference:	Blu-ray File System Specifications
Default Program Action:	Error

Rule ID: 835

File not allocated at the inner radius area

A file that is recommended to be allocated at the inner radius was found at the outer radius instead.

Background

For redundancy purposes, the Blu-ray specifications recommend that certain files and their backups be recorded at the inner radius and outer radius, respectively. In this case, this rule is specific to Database files and their backups (index.bdmv, MovieObject.bdmv, xxxxx.mpls, zzzzz.clpi, sound.bdmv and aaaaa.otf, where: aaaaa, xxxxx and zzzzz indicate a 5-digit number).

Additional Info

When this rule is triggered, the Additional Info column in the Analysis will identify the file in question.

Original Database File "[*DatabaseFileName*]**"**

This message is triggered when the original Database file is recorded at the outer radius of a Blu-ray disc. The Blu-ray specifications recommend that, for robustness and playback performance, the original Database files should be recorded at the inner radius and it backup files at the outer radius.

Severity

It is not a requirement by the Blu-ray specifications that these files be recorded at the inner or outer radius. It is only a recommendation. Therefore, this rule is only a WARNING.

Cause

This problem is caused by the authoring system that created the image.

Solution

If it is required for these files to be recorded at the inner or outer radius, then the image must be re-authored.

Type:	UDF
Reference:	System Description Blu-ray Disc Read-Only Format Part 2: File System Specification (UDF) Version 1.2
Default Program Action:	Warning

Rule ID: 810

File not allocated at the outer radius area

A file that is recommended to be allocated at the outer radius was found at the inner radius instead.

Background

For redundancy purposes, the Blu-ray specifications recommend that certain files and their backups be recorded at the inner radius and outer radius, respectively. In this case, this rule is specific to Database files and their backups (index.bdmv, MovieObject.bdmv, xxxxx.mpls, zzzzz.clpi, sound.bdmv and aaaaa.otf, where: aaaaa, xxxxx and zzzzz indicate a 5-digit number).

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will identify the file in question.

Backup Database File "[*DatabaseFileName*]"

This message is triggered when the backup Database file is recorded at the inner radius of a Blu-ray disc. The Blu-ray specifications recommend that, for robustness and playback performance, the original Database files should be recorded at the inner radius and it backup files at the outer radius.

Severity

It is not a requirement by the Blu-ray specifications that these files be recorded at the inner or outer radius. It is only a recommendation. Therefore, this rule is only a WARNING.

Cause

This problem is caused by the authoring system that created the image.

Solution

If it is required for these files to be recorded at the inner or outer radius, then the image must be re-authored.

Type:	UDF
Reference:	System Description Blu-ray Disc Read-Only Format Part 2: File System Specification (UDF) Version 1.2
Default Program Action:	Warning

Rule ID: 811

File not allocated contiguously

The BD-ROM file system specifications require that Gathered files be recorded contiguously. When this rule is triggered, the Additional Info column in the Analysis will display the file in question.

Type:	UDF
Reference:	BD-ROM U05-023
Default Program Action:	Warning

Rule ID: 807

File not found

The EclipseSuite tools were unable to locate a required file.

Background

The Blu-ray specifications each require certain files to be present on an image. Some files are part of the audio/video specifications while others are required only when the AACS encryption is applied to an image.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will identify the file that triggered this error.

Blu-ray Video: '\BDMV\index.bdmv'

The index.bdmv is one of the primary Blu-ray files, which is essential in the playback of a Blu-ray Video.

Blu-ray Video: '\AACS\Unit_Key_RO.inf'

This file stores all CPS Unit Keys (encryption keys) required for AACS encryption and decryption.

Blu-ray Video: '\BDMV\MovieObject.bdmv'

The MovieObject.bdmv is one of the primary Blu-ray files, which is essential in the playback of a Blu-ray Video.

Blu-ray Video: '\AACS\CPSUnitXXXXX.cci'

This is a CPS Usage file which describes the CCI and related information of each CPS Unit. Each CPS Unit has an associated CPS Usage File named CPSUnitXXXXX.cci where XXXXX is a 5-digit number which is equal to the CPS Unit number that the CCI file is associated. For example, CPS Unit 1 will have the associated CCI file CPSUnit00001.cci.

CBDPlayer: ClipInfo file '\BDMV\CLIPINF\*.clpi' not found for '[*Filename*]'

The clip information file (.clpi) is required for every Clip AV Stream file as it provides time stamps of the access points into the corresponding AV stream file.*

\BDMV\JAR\nnnnn.jar

The specified JAR file is missing.

\CERTIFICATE\id.bdmv

The file 'id.bdmv' failed to load (missing?).

\CERTIFICATE\online.crt

The online certificate file is missing.

\CERTIFICATE\online.sig

The online signature file is missing.

\CERTIFICATE\online.crl

The online content revocation list file is missing.

\CERTIFICATE\app.discroot.crt

The application root certificate file is missing.

Blu-ray Video: '[*Filename*]'

This message is displayed when the files \AACS\Unit_Key_RO.inf or \AACS\DUPLICATE\Unit_Key_RO.inf are not found. The Unit_Key_RO.inf file stores all CPS Unit Keys (encryption keys) required for AACS encryption and decryption. The file is stored in the AACS folder and a backup copy in the DUPLICATE folder.

Severity

Since this rule is triggered when required files are missing, it is likely that any missing required file will cause playability problems. It is for this reason that this rule defaults to an ERROR.

Cause

This problem is cause by the system that authored the image.

Solution

The image must be re-authored.

Type:	UDF
Reference:	None
Default Program Action:	Error

Rule ID: 830

File not in Authoring Studio namespace

The explanation for this title check rule contains confidential information. Please refer to the studio-specific supplemental rules help PDF document. The document is available from Eclipse Support.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

Rule ID: 1674

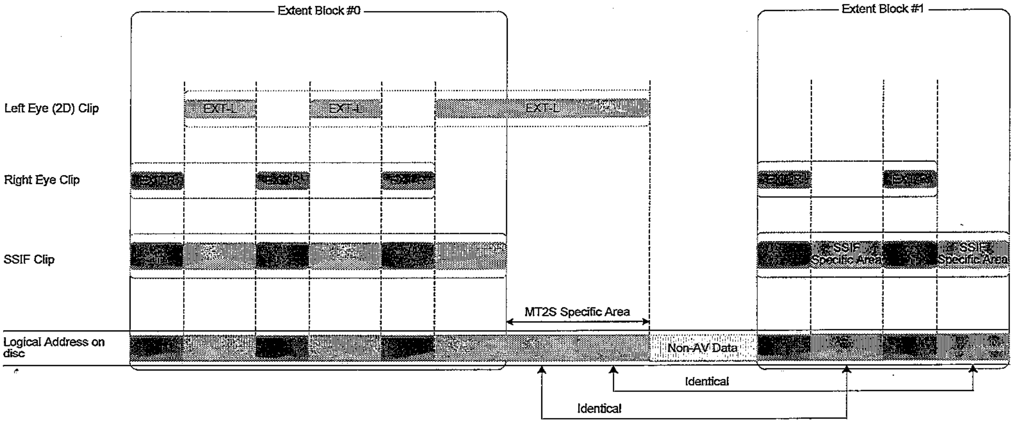
First SPN for 3D clip extent differs

The first source packet number of a 3D Clip extent does not match the actual source packet number found.

Background

There is a Clip Information file (zzzzz.clpi) for each Clip AV Stream file (zzzzz.m2ts). The ClipInfo file describes the contents of the AV Stream file. There is also a ClipInfo file for the 3D SSIF AV Stream file.

The SSIF file is constructed from extents from the left and right eye M2TS AV Stream files. The first sector of each extent in the SSIF file must be the start of source packet. The first sector of a source packet includes a number identifier which increments sequentially for subsequent source packets within each extent. The source packet number (SPN) of the first source packed in each extent is stored in a table inside the corresponding ClipInfo file. During the analysis, the EclipseSuite tools verify that the source packet number stored in this table matches with the corresponding source packet number of the first source packet of an extent. If they are not the same then this error is triggered.


Extent Block #0
Extent Block #1
Left Eye (2D) Clip
EXT-L
EXT-L
EXT-L
Right Eye Clip
EXT-R
EXT-R
EXT-R
EXT-R
EXT-R
SSIF Clip
SSIF Specific Area
SSIF Specific Area
MT2S Specific Area
Logical Address on disc
Non-AV Data
Identical
Identical

Additional Info

When this condition occurs, the **Additional Info** column in the Analysis will identify the extent, expected and actual source pack number and ClipInfo file.

Severity

This is a requirement for 3D. It is unknown how this may affect playability. Therefore, it is treated as an ERROR.

Cause

This condition is caused by the authoring system that created the image.

Solution

The image must be re-authored. Contact Eclipse Customer Support for further assistance.

Type:	3D
Reference:	3D Specifications
Default Program Action:	Error

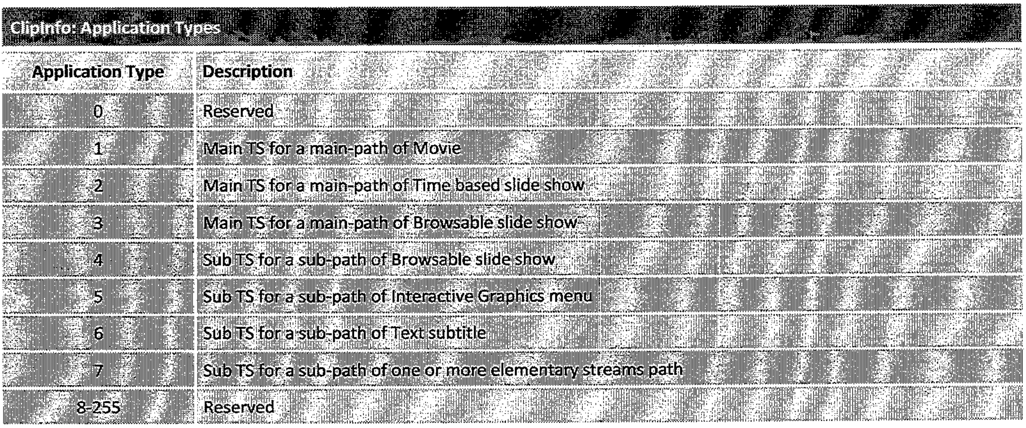
Rule ID: 1754

HDMV transport stream PAT interval exceeded

The PAT (Program Association Table) appears more than once in a Transport Stream.

Background

For each Clip AV Stream file there is a corresponding Clip Information file, which describes the properties of the Clip AV Stream file. Among other things, the Clip Information file describes the different types of audio and video that is stored in the Clip AV Stream file. The Clip Info file includes a field that identifies an application type using the Clip. This field also indicates constraints on the Clip and on the PlayList which references the Clip.



ClipInfo: Application Types

Application Type	Description
0	Reserved
1	Main TS for a main-path of Movie
2	Main TS for a main-path of Time based slide show
3	Main TS for a main-path of Browsable slide show
4	Sub TS for a sub-path of Browsable slide show
5	Sub TS for a sub-path of Interactive Graphics menu
6	Sub TS for a sub-path of Text subtitle
7	Sub TS for a sub-path of one or more elementary streams path
8-255	Reserved

All Transport Streams contain a PAT (Program Association Table), PMT (Program Map Table) and SIT (Selection Information Table). The specifications impose certain restrictions on these tables based on the Clip Info application type. For an application type 6, these tables are required to appear only once at the beginning of the Transport Stream. It also specifies that these tables also have a maximum time interval of 100 milliseconds. This rule indicates that the PAT appeared more than once or that it exceeded 100 millisecond time interval.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display more details.

'[*nnnnn*].m2ts': PAT can only appear once when ClipInfo application type is 6

This message indicates that the PAT appears more than once in the Transport Stream. The specifications indicate that it should only appear once at the beginning of the Transport Stream.

'[*nnnnn*].m2ts': actual ([*Time*]) milli-second, expected maximum (100) milli-second

This message indicates that the PAT exceeded the maximum time interval of 100 milliseconds.

Severity

It is unknown how this will affect playability. Therefore, it is considered an ERROR.

Cause

This problem is typically caused by the authoring system that created the image.

Solution

The image must be re-authored.

Type: Blu-ray

Reference:	Blu-ray Disc Read-Only Format Part 3: Audio Visual Specifications (3-1 Core Specifications)
Default Program Action:	Error

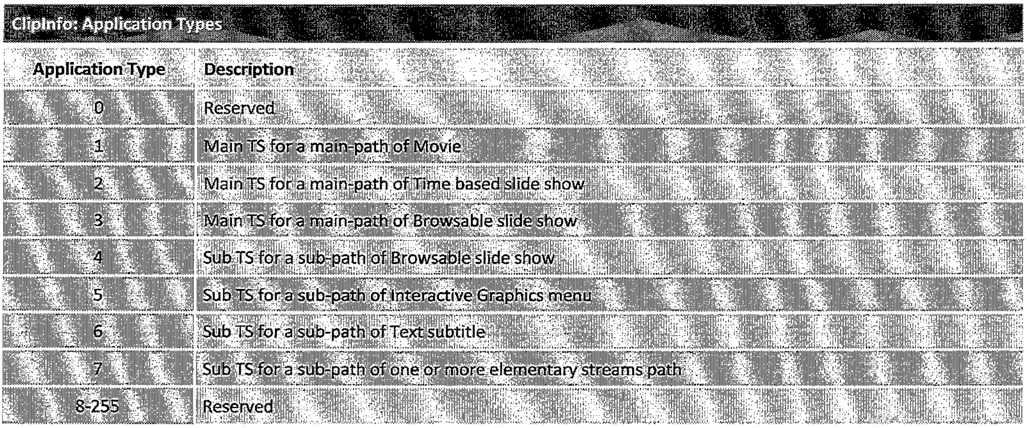
Rule ID: 1646

HDMV transport stream PMT interval exceeded

The PMT (Program Map Table) appears more than once in a Transport Stream.

Background

For each Clip AV Stream file there is a corresponding Clip Information file, which describes the properties of the Clip AV Stream file. Among other things, the Clip Information file describes the different types of audio and video that is stored in the Clip AV Stream file. The Clip Info file includes a field that identifies an application type using the Clip. This field also indicates constraints on the Clip and on the PlayList which references the Clip.



ClipInfo: Application Types

Application Type	Description
0	Reserved
1	Main TS for a main-path of Movie
2	Main TS for a main-path of Time based slide show
3	Main TS for a main-path of Browsable slide show
4	Sub TS for a sub-path of Browsable slide show
5	Sub TS for a sub-path of Interactive Graphics menu
6	Sub TS for a sub-path of Text subtitle
7	Sub TS for a sub-path of one or more elementary streams path
8-255	Reserved

All Transport Streams contain a PAT (Program Association Table), PMT (Program Map Table) and SIT (Selection Information Table). The specifications impose certain restrictions on these tables based on the Clip Info application type. For an application type 6, these tables are required to appear only once at the beginning of the Transport Stream. It also specifies that these tables must also have a maximum time interval of 100 milliseconds. This rule indicates that the PMT appeared more than once or that it exceeded 100 millisecond time interval.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display more details.

'[*nnnnn*].m2ts': PMT can only appear once when ClipInfo application type is 6

This message indicates that the PMT appears more than once in the Transport Stream. The specifications indicate that it should only appear once at the beginning of the Transport Stream.

'[*nnnnn*].m2ts': actual ([*Time*]) milli-second, expected maximum (100) milli-second

This message indicates that the PMT exceeded the maximum time interval of 100 milliseconds.

Severity

It is unknown how this will affect playability. Therefore, it is considered an ERROR.

Cause

This problem is typically caused by the authoring system that created the image.

Solution

The image must be re-authored.

Type:	Blu-ray
Reference:	Blu-ray Disc Read-Only Format Part 3: Audio Visual Specifications (3-1 Core Specifications)
Default Program Action:	Error

Rule ID: 1647

High Definition image missing UDF

The ImageEncoder was unable to find the UDF file system on the image and, therefore, is unable to mount it to complete the AACS processing during mastering. The job will abort.

Background

Mastering of a Blu-ray image is typically done from a Type C image. During mastering, the encoder must perform one final change in the image and that is to encrypt the Unit_Key_RO.Inf file. In order to encrypt the file, the encoder must first find out where it is located. To do this, the encoder must parse the UDF file system. Once the UDF file system is 'mounted', the file can be located the encryption can take place.

NOTE
The encryption of the Unit_Key_RO.Inf file is performed as the data is being processed in memory. The file in the original user data file (UD.DAT) is never changed.

Severity

This is a serious problem since it indicates that the encoder is unable to master the image.

Cause

This error occurs when the ImageEncoder is unable to find the UDF file system on the image. Additional errors and/or warnings may appear providing more details as to why the UDF was not found.

Solution

This error is used to indicate that an image cannot be processed because the UDF file system was not found. It does not indicate why UDF was not found. The solution to this problem is dependent on the reason why the UDF file system was not found. Please check any additional errors and/or warnings that might be related to this failure. For further assistance, contact Eclipse Customer Support.

Type:	Exclusion
Reference:	N/A
Default Program Action:	Error

Rule ID: 1474

High Definition processing halted

Analysis of a BD image has aborted.

Background

There are certain conditions that may cause the analysis operation to abort and not display the error condition in the analysis tab. When this happens, the analysis results are misleading since the error that caused the abort is not shown in the analysis. This problem becomes more serious in ImageCopy when it is being run via IEScheduler, RemoteScheduler or ImageNet Scheduler. The reason is that these programs are the main user interface. If the abort condition occurs, these programs will show the user an indication that the job completed without problems. A change in the EclipseSuite analysis engine was done so that such conditions are detected, then this rule is triggered.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display the specific reason why it aborted with one of the following messages.

- Error mounting UDF
- Error mounting UDF - Video Navigation Error
- AACS Decryption Error
- AACS Encryption Error
- [Error string]
- [Error number]

Contact Eclipse Customer Support for further assistance.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Abort

Rule ID: 1527

History of ImageArchive BD record found in BDCMF

This is an informational message that identifies whether a BDCMF image includes process history which indicates that the image has been previously archived to a database.

Background

When the BD Archive option is used, the Content Certificate Management Utility (CMU) automatically archives Type C images to a database. During this process, the CMU will add an entry into the process history of the BDCMF.CMF file, indicating that the image has been archived. This message indicates that the process history includes an entry that specifies that the image is archived.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Flag

Rule ID: 1880

ImageArchive BD base directory does not match target

The folder that a Blu-ray image is being restored to is different from the original folder when the image was archived.

Background

When ImageArchive BD archives an image, it stores the original image folder where the image was located at the time or archiving. When the image is later restored, it is re-created as a BDCMF Type C. Although the user can specify any output folder, in some cases, the folder is used to uniquely identify the image. In such cases, this rule is used to alert the user, that the image may be getting restored to the wrong folder. ImageCopy will prompt the user whether it should continue and if so, trigger the rule "ImageArchive BD base directory overridden".

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Flag

Rule ID: 1893

ImageArchive BD base directory overridden

During a restore operation, the user chose to restore the image to a folder that was different from the original from which the image was archived.

Background

When ImageArchive BD archives an image, it stores the original image folder where the image was located at the time or archiving. When the image is later restored, it is re-created as a BDCMF Type C. Although the user can specify any output folder, in some cases, the folder is used to uniquely identify the image. In such cases, the rule **"ImageArchive BD base directory does not match target"** is used to alert the user, that the image may be getting restored to the wrong folder. ImageCopy will prompt the user whether it should continue and if so, triggers this rule.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Flag

Rule ID: 1894

Image Constraint Token disabled

The Image Constraint Token flag is disabled indicating that the video from the analog outputs will be down-sampled to a resolution slightly higher than a DVD-Video.

Background

Image Constraint Token is part of the AACS copy protection system and is enforced through the **High-bandwidth Digital Content Protection (HDCP)** system on devices which support DVI and HDMI. This flag is used for down-sampling of the high definition video of a Blu-ray Video image to a resolution slightly higher than DVD-Video.

Some early HDTVs did not support HDCP. Therefore, enabling this flag would result in a video resolution that is not high definition. Because of this, movie studios have reportedly agreed to delay the use of this flag.

On a Blu-ray Video image, the Image Constraint Token flag is specified in the CPS Unit Usage file of each CPS Unit.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will identify the CPS Unit number for which this rule was triggered.

Severity

This condition does not indicate a problem as long as full 1080p video via the analog outputs was intended. Therefore, it is only considered a Flag.

Cause

This flag is set during authoring of the image.

Solution

This condition can be ignored as long as the author/customer wanted the video to be constrained when played via the analog outputs. Since this is a rare condition, you should consult with the customer or author to confirm this is what was intended.

Type:	Blu-ray
Reference:	AACS Specifications for Blu-ray
Default Program Action:	Flag

Rule ID: 1712

Image signature mismatch

The EclipseSuite tools detected that the signature did not match the image being analyzed.

If a DVD image includes a signature, it will be re-calculated every time the image is analyzed, copied or verified. When the EclipseSuite tools finish analyzing the image, the calculated signature is compared with the original signature. If they are not the same, then this error is triggered.

This error would indicate the possibility that the signature and the image are not a matching pair. However, if that was the case, there should be additional errors such as data comparison errors in the case of ImageVerify. It is also possible that the image has become corrupt. This can occur when an image is transferred over a network, or if the image becomes corrupt due to hard disk problems.

Copy Protections

When the ImageSignature is first created by ImageCopy, the image is analyzed to see if it contains a copy protection. Detection of any copy protection is important since it will affect the signature that is created. ImageCopy will automatically generate the proper signature for images that include the CSS copy protection. For any other copy protection, ImageCopy must be configured with the proper Plug-In so that the copy protection is detected and the correct is signature generated.

For example, the Macrovision RipGuard copy protection Plug-In is not absolutely required when the image is loaded with ImageCopy. However, most premastering facilities do configure it so that RipGuard images are identified and proper signatures are generated.

If ImageCopy is not configured with the RipGuard Plug-In, ImageCopy still loads the image and generates a signature. During verification, ImageVerify must be configured with the RipGuard Plug-In in order to perform a proper verification. If ImageVerify if configured for ImageSignatures, the signature generated by ImageVerify will skip sectors that are protected with RipGuard. This generates a different signature from the original that was generated by ImageCopy. The result is this error message.

Type:	Other
Reference:	None
Default Program Action:	Error

Rule ID: 331

Image Source CMF Type not allowed with current configuration

ImageEncoder has detected a Blu-ray image type that it cannot master. The mastering process will abort.

Background

Initially, it was required that encoders master from Blu-ray Type D images only. Therefore, by default, the Eclipse ImageEncoder would block mastering of any other image Type.

When this restriction was lifted, Eclipse added a registry entry to allow mastering of Type C images. The registry setting was supposed to be temporary until testing ensuring that mastering of Type C images worked without problem. However, this registry setting remained a requirement for ImageEncoder.

With the introduction of the new Sony RIT-2000 ROM Mark Inserter, it is no longer recommended mastering from a Type D image. Therefore, Eclipse's ImageEncoder will block mastering from this type of images.

Additional Info

When this rule is triggered, the **Additional Info** column in the analysis will display more details with one of the following messages.

Type C

BETA Versions of ImageEncoder prior to 3.0 Beta Z5 require a registry setting to allow mastering of Type C images. This message indicates that the image is Type C and that the version of ImageEncoder you are running is configured to block mastering of these images.

You can create the registry entry with the information below. However, we recommend that you contact Eclipse for an upgrade to the ImageEncoder software instead since this restriction has been removed in later versions.

Registry Key
\HKEY_CURRENT_USER\Software\Eclipse\ImageEncoder\EncoderSettings

Registry Value
Type: REG_DWORD
Name: AllowTypeCBD
Data Value: 0 (to block Type C images) or 1 (to allow Type C images)

Type A and B

This message indicates that the image is Type A or Type B with AACS. ImageEncoder is not able to master from these types of images. It must be at least a Type C.

Type C1 and D

This message indicates that the image is Type C1 or Type D and that the Sony RIT-2000 ROM Mark Inserter unit is being used. Mastering of these types of images is not possible when using this system.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

Rule ID: 1453

ImageArchive BD base directory does not match target

The output directory of an ImageArchive BD restore operation does not match with the original directory from which the image was archived.

Background

When a Blu-ray image is archived to a database using the ImageArchive BD option, the original folder where the image was located is also stored in the database. During a restore operation, a replica is used to 'restore' the original image back onto the hard disk. If the operator specifies a different output directory from the original stored on the database, then he/she is alerted and must confirm whether this was intended or whether the restore operation should be aborted.

Severity

This rule is only informational to indicate that the user has entered a different directory name from the one that was originally archived. However, if the directory name is used as a unique identifier of the image, then you may choose to make this an error.

Cause

This rule is triggered when the user specified a different output directory from the original when the image was archived.

Solution

You do not have to do anything unless the folder name must match the original; in which case this rule should be changed to an ERROR.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Flag

Rule ID: 1893

ImageArchive BD base directory overridden

The output directory of an ImageArchive BD restore operation does not match with the original directory from which the image was archived and the operator has chosen to continue as is.

Background

When a Blu-ray image is archived to a database using the ImageArchive BD option, the original folder where the image was located is also stored in the database. During a restore operation, a replica is used to 'restore' the original image back onto the hard disk. If the operator specifies a different output directory from the original stored on the database, then he/she is alerted and must confirm whether this was intended or whether the restore operation should be aborted. This rule indicates that the operator chose to continue as is.

Severity

This rule is only informational to indicate that the user has chosen to continue with a different directory name in the restore operation. However, if the directory name is used as a unique identifier of the image, then you may choose to make this an error.

Cause

This rule is triggered when the user specified a different output directory from the original when the image was archived. ImageCopy prompts whether it should abort or continue. This rule indicates the operator chose to continue as is.

Solution

You do not have to do anything unless the folder name must match the original; in which case this rule should be changed to an ERROR.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Flag

Rule ID: 1894

ImageArchive BD record found

This is an informational message that indicates that an archive database record was found for the image being analyzed.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Flag

Rule ID: 1878

ImageArchive BD record not found

This is an informational message that indicates that an archive database record was not found for the image being analyzed.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Flag

Rule ID: 1879

Incorrect allocation order for Stereoscopic Interleaved files

The allocation order of extents of the SSIF file is incorrect.

Background

A Stereoscopic Interleaved file (SSIF) consists of extents from a 2D Clip AV file left eye (*.m2ts) and a Clip AV file for the right eye. The extents are interleaved in an order defined by the Blu-ray specifications for 3D. This condition indicates that the order of the extents is incorrect. The order of the extents is required for seamless playback.

Severity

It is unknown how this condition may affect playability. Therefore, it is treated as an ERROR.

Cause

This condition is caused by the authoring system that created the image.

Solution

The image must be re-authored. Contact Eclipse Support for further assistance.

Type:	3D
Reference:	Blu-ray Specifications Annex P: Main requirements for Stereoscopic 3D
Default Program Action:	Error

Rule ID: 1762

Incorrect BDCMF ImageData file size

The file size specified in BDCMF does not match the actual file size.

Background

During analysis of a Blu-ray image, the EclipseSuite tools validate many of the fields in the BDCMF.CMF file of a Blu-ray image. Part of the validation includes checking the size of all files that make up the BDCMF image file-set. The BDCMF.CMF file includes a section where all of the BDCMF files and their details are specified. Each file entry includes its file size. The EclipseSuite tools determine the actual size of each file then compare it to the size stored in the BDCMF.CMF file. If the size specified in the BDCMF.CMF file and the actual size do not match then this rule is triggered.

The BDCMF.CMF file contains the details on the files that make up a BDCMF image file-se. File details are stored in the ImageData XML element as shown in the example below.

```
...
<ImageData>
    <File Type="PICData" Name="PIC.DAT" Size="65536">
        <HashValue HashType="SHA-1">1234123412341234123412341234123412341234</HashValue>
    </File>
    <File Type="PACDataLayer0" Name="PACL0.DAT" Size="65536">
        <HashValue HashType="SHA-1">4123412341234123412341234123412341234123</HashValue>
    </File>
    <File Type="UserControlData" Name="UCD.DAT" Size="75857472">
        <StartPSN>00100000</StartPSN>
        <HashValue HashType="SHA-1">3412341234123412341234123412341234123412</HashValue>
    </File>
    <File Type="UserData" Name="UD.DAT" Size="8630894592">
        <StartPSN>00100000</StartPSN>
        <HashValue HashType="SHA-1">2341234123412341234123412341234123412341</HashValue>
    </File>
</ImageData>
```

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will identify the file and the size differences with the following message.

File '[*Filename*]'. Expected [*ExpectedSize*]. Actual [*ActualSize*]

This message identifies the file that triggered this rule. It also shows the different in sizes.

Severity

The severity of this rule is only a WARNING since it does not affect the EclipseSuite tools. In addition, if you are using ImageCopy 6.0 Beta Z33 later to encrypt the image, this problem is corrected automatically on the output image.

Cause

This problem is typically caused by the authoring system that created the image.

Solution

Use ImageCopy 6.0 Beta Z33 or later to encrypt the image so that this problem can be corrected on the output image. If not using ImageCopy then the image may have to be re-authored as some systems rely on the correct file size values that are specified in the BDCMF file.

Type:	Blu-ray
Reference:	BDCMF Specifications
Default Program Action:	Warning

Rule ID: 1564

Incorrect CC Digest Value

A value in the Content Certificate does not match the recalculated value.

Background

To protect a file's integrity, the Blu-ray Video format requires that certain files be protected by means of Content Hashing (e.g. ClipAV files). Files are divided into Hash Units, each consisting of 96 consecutive logical sectors. A hash value is then calculated on each Hash Unit and it is stored as an entry in the Content Hash Table (CHT). The hash entries in the Content Hash Tables are also hashed and the value is stored in the Content Certificate (CC) file as Digest entries.

During the analysis of BD images, the Eclipse software recalculates all hashes. It compares the recalculated hash and digest values to those already in the CHT and CC files, respectively. This rule is triggered if any of the recalculated hash and digest values don't match.

The Content Certificate files are recorded in the \AACS directory and a backup copy in the \AACS\DUPLICATE directory. There is a Content Certificate file for the files in each layer. On a single layer and layer 0 of a dual-layer image, the filename is "Content000.cer". The filename for the files in layer 1 is "Content001.cer".

Similarly, the Content Hash Table files are also recorded in the \AACS directory and a backup in the \AACS\DUPLICATE directory. The filenames for a single layer and layer 0 of a dual-layer image is "ContentHash000.tbl. The filename for the files in layer 1 is "ContentHash001.tbl".

Additional Info

When this rule is triggered, the Additional Info column will display one of the following messages indicating the specific cause of this error.

Layer [LayerNo] Hash Digest at offset [Offset] actual (ActualValue) Expected (ExpectedValue)

This message is displayed when the calculated Content Hash Table Digest values do not match the Digest values already recorded in the Content Certificate file.

If the values don't match it is an indication that the file may be corrupt or that bad calculation was performed during the analysis of the image or when the original hash values were calculated and stored in the CC and CHT. Either way, it is a condition which may result in playability problems.

unable to load duplicate content certificate

This message is displayed when an error occurs while attempting to load the duplicate Content Certificate file for layer 0 (\AACS\Duplicate\Content000.cer).

During analysis of a BD image, the file is loaded into memory in order to compare the hash values recorded in it to the calculated values during the analysis.

This message indicates a problem when reading the file. There may not be enough memory, an invalid file address or a file read error.

unable to access duplicate content certificate

This message is displayed when an error occurs while attempting to load the duplicate Content Certificate file for layer 0 (\AACS\Duplicate\Content000.cer).

During analysis of a BD image, the file is loaded into memory in order to compare the hash values recorded in it to the calculated values during the analysis.

This message indicates a problem reading the file. The file was not found.

unable to load L1 duplicate content certificate

This message is displayed when an error occurs while attempting to load the duplicate Content Certificate file for layer 0 (\AACS\DUPLICATE\Content001.cer).

During analysis of a BD image, the file is loaded into memory in order to compare the hash values recorded in it to the calculated values during the analysis.

This message indicates a problem when reading the file. There may not be enough memory, an invalid file address or a file read error.

unable to access L1 duplicate content certificate

This message is displayed when an error occurs while attempting to load the duplicate Content Certificate file for layer 0 (\AACS\DUPLICATE\Content001.cer).

During analysis of a BD image, the file is loaded into memory in order to compare the hash values recorded in it to the calculated values during the analysis.

This message indicates a problem reading the file. The file was not found.

Layer 0 Hash Digest at offset [Offset] actual (*ActualValue*) Expected (*ExpectedValue*)

This message is displayed when the calculated Content Hash Table Digest values do not match the Digest values already recorded in the Content Certificate file for layer 0 (Content000.cer).

If the values don't match it is an indication that the file may be corrupt or that bad calculation was performed during the analysis of the image or when the original hash values were calculated and stored in the CC and CHT. Either way, it is a condition which may result in playability problems.

Layer 1 Hash Digest at offset [Offset] actual (*ActualValue*) Expected (*ExpectedValue*)

This message is displayed when the calculated Content Hash Table Digest values do not match the Digest values already recorded in the Content Certificate file for layer 1 (Content001.cer).

If the values don't match it is an indication that the file may be corrupt or that bad calculation was performed during the analysis of the image or when the original hash values were calculated and stored in the CC and CHT. Either way, it is a condition which may result in playability problems.

Severity

This error is considered serious since it may lead to playability problems.

NOTE
Blu-ray players are required to verify at least 1% of the hash units. Blu-ray players may randomly select the hash units to verify.

Cause

These problems are typically caused by invalid hash and digest values in the Content Hash Table and Content Certificate files.

On a Type A image, these files do not contain any data. However, they are updated during the encryption process (e.g. conversion from Type A to Type B). Therefore, the problem is typically caused by the utility that generated these values and stored them into the Content Hash Table and Content Certificate files.

Solution

If the Type A image is still available, it may be possible that the image can be re-encrypted and signed using the same CC and MKB Order files. Contact Eclipse Support for further assistance.

Type:	Main Channel
Reference:	AACS Specifications for Blu-ray
Default Program Action:	Error

Rule ID: 858

Incorrect CC Header

Fields in the Content Certificate file header do not match with the calculated or expected values.

Background

There is a Content Certificate file on each layer of a BD image. On a single layer image and layer 0 of a dual-layer image, the filename is CONTENT000.CER. On layer 1 it is CONTENT001.CER. Both files contain Digest entries for the hashes in the Content Hash Tables. The Content Certificate files include a header at the beginning of the file. This header provides information about the image.

Both files are stored in the "\AACS" folder. There is also a duplicate copy of both files in the "\AACS\DUPLICATE" folder.

Additional Info

When this error occurs, the **Additional Info** column in the analysis will display more details about the error with one of the following messages.

Layer [*n*] Field: Certificate Type actual ([*CC type*]), expected ([*CC type*])

The Certificate Type field contains an invalid value. According to the AACS Specifications, the Certificate Type must be set to 0000h.

Since a dual-layer image includes a content certificate file for each layer, this message also specifies the layer number in order to identify the file that has this problem: CONTENT000.CER for layer 0 (or single layer) image and CONTENT001.CER for layer 1.

Layer [*n*] Field: Total_Number_of_HashUnits actual ([# *of hash units*]), expected ([*calculated value*])

This message indicates that the calculated total number of hash units does not match the value in specified the content certificate file. The total number of hash units is the sum of all hash units on the image (both layers combined).

Since a dual-layer image includes a content certificate file for each layer, this message also specifies the layer number in order to identify the file that has this problem: CONTENT000.CER for layer 0 (or single layer) image and CONTENT001.CER for layer 1.

Layer [*n*] Field: Total_Number_of_Layers actual ([# *of layers*]), expected ([*expected*])

This message indicates that the actual number of layers does not match the value specified in the content certificate file. The total number of layers in the content certificate file should match with the number of layers specified in the CMF file set.

Since a dual-layer image includes a content certificate file for each layer, this message also specifies the layer number in order to identify the file that has this problem: CONTENT000.CER for layer 0 (or single layer) image and CONTENT001.CER for layer 1.

Layer [*n*] Field: Layer_Number actual ([*layer* #]), expected ([*expected*])

This message indicates that the actual layer number does not match the value specified in the content certificate file. The layer number specified in the file should match the file itself. For example, the file CONTENT000.CER should have the value '0' in the Layer_Number field. Similarly, the file CONTENT001.CER should have the value '1'.

Since a dual-layer image includes a content certificate file for each layer, this message also specifies the layer number in order to identify the file that has this problem: CONTENT000.CER for layer 0 (or single layer) image and CONTENT001.CER for layer 1.

Layer [*n*] Field: Number_of_HashUnits (on layer) actual ([# *of hash units*]), expected ([*expected value*])

This message indicates that the number of hash units on a layer does not match with the specified value in the content certificate file for that layer.

Each content certificate file contains digest entries for all the hash units in the layer it represents. The value for the total number of hash units in each layer is stored in the Number_of_HashUnits field in the header of each content certificate file.

Since a dual-layer image includes a content certificate file for each layer, this message also specifies the layer number in order to identify the file that has this problem: CONTENT000.CER for layer 0 (or single layer) image and CONTENT001.CER for layer 1.

Layer [*n*] Field: Number_of_Digests (on layer) actual ([# *of digests*]), expected ([*expected value*])

This message indicates that the number of Clip AV Stream Files recorded on a layer does not match with the specified value in the content certificate file for that layer. The Number_of_Digests value specifies the number of Clip AV Stream Files which have a file size equal to or greater than 96 logical sectors on a layer.

Since a dual-layer image includes a content certificate file for each layer, this message also specifies the layer number in order to identify the file that has this problem: CONTENT000.CER for layer 0 (or single layer) image and CONTENT001.CER *for layer 1.*

Layer [*n*] Field: Length_Format_Specific_Section actual ([*actual value*]), expected ([*expected value*])

This message indicates that the value specified in the Length_Format_Specific_Section field does not match the actual length of the Format_Specific_Section field in the content certificate file header.

Since a dual-layer image includes a content certificate file for each layer, this message also specifies the layer number in order to identify the file that has this problem: CONTENT000.CER for layer 0 (or single layer) image and CONTENT001.CER for layer 1.

Layer [*n*] Field: Num_of_CPS_Unit actual ([*actual no. of cps units*]), expected ([*calculated value*])

The number of CPS Units differs between the content certificate file and the calculated value.

Type:	Blu-ray
Reference:	AACS Blu-ray Disc Pre-recorded Book 0.912
Default Program Action:	Error

Rule ID: 884

Incorrect CHT Header

This Blu-ray error indicates that there is a problem with the starting hash unit number, the hash unit offset, the clip number, or the number of hash entries on the layer. This information is recorded in the AACS Content Hash Table Headers.

Background

For each physical layer of BD-ROM, the Content Hash Table (CHT) is stored in the "\AACS" and "\AACS\DUPLICATE" directories. A single-layer disc has a single file named "ContentHash000.tbl", while a dual-layer disc has two files names "ContentHash000.tbl" for Layer 0 and "ContentHash001.tbl" for Layer 1. The Layer 0 and Layer 1 hash tables each need to be stored on the respective physical layer.

The Content Hash Table contains a hash value for each hash unit of the Clip AV Stream file in the corresponding layer, along with header information, and must be formatted according to the specification. The Eclipse tools report any inconsistencies between the Content Hash Table headers and the data contained on the media. This information is also used to create and validate the Content Certificate.

Additional Info

The specific header in the CHT that is in error will be reported in the **Additional Info** column in the Analysis tab.

Layer [*n*] clip [*Clip #####*] Field: Starting_HU_Num actual ([*Starting_HU_Num in header*]), expected ([*Starting_HU_Num found*])

The field Starting_HU_Num indicates the position in hash units of the first hash value of a Clip AV Stream file.

The CHT header maintains a list of all hash units for each layer. Starting_HU_Num is an index into this list and identifies the first hash unit of a Clip AV file.

On a single layer image, the starting hash unit number for any Clip AV file should always be 0. On a dual-layer image, if the Clip AV file does not span into layer 1, then the starting hash unit in the CHT for that file is also 0. If the file spans into layer 1, then the starting hash unit number in layer 1 is equal to the number of hash units on layer 0, for the same file.

This message identifies the following items:

***n:** The layer in which the error occurred. Knowing the layer number gives you the CHT file where the error occurred (Single/Layer 0: ContentHash000.tbl or Layer 1: ContentHash001.tbl).*

***Clip #####:** This identifies the AV file that is affected by this error (#####.m2ts).*

***Starting_HU_Num in header:** The starting hash unit number in the CHT header for the Clip AV file #####.m2ts.*

***Starting_HU_Num found:** The starting hash unit number that was calculated by the EclipseSuite tools for the Clip AV file #####.m2ts.*

Layer [*n*] clip [*Clip #####*] Field: HU_Offset_in_Clip actual ([*HU_Offset_in_Clip in header*]), expected ([*HU_Offset_in_Clip found*])

The field Starting_HU_Num indicates the position in hash units of the first hash value of a Clip AV Stream file.

The CHT header maintains a list of all hash units for each layer. Starting_HU_Num is an index into this list and identifies the first hash unit of a Clip AV file.

On a single layer image, the starting hash unit number for any Clip AV file should always be 0. On a dual-layer image, if the Clip AV file does not span into layer 1, then the starting hash unit in the CHT for that file is also 0. If the file spans into layer 1, then the starting hash unit number in layer 1 is equal to the number of hash units on layer 0, for the same file.

This message identifies the following items:

***n:** The layer in which the error occurred. Knowing the layer number gives you the CHT file where the error occurred (Single/Layer 0: ContentHash000.tbl or Layer 1: ContentHash001.tbl).*

***Clip #####:** This identifies the AV file that is affected by this error (#####.m2ts).*

***Starting_HU_Num in header:** The starting hash unit number in the CHT header for the Clip AV file #####.m2ts.*

***Starting_HU_Num found:** The starting hash unit number that was calculated by the EclipseSuite tools for the Clip AV file #####.m2ts.*

Layer [*n*] Field: Clip_Num actual ([*actual clip #*]), expected ([*expected*])

The clip number in the CHT header does not match with the filename's number (e.g. 00001.m2ts).

Layer [*n*] Image clip [*clip #*] number of hash entries actual ([*actual # of hash entries*]), expected ([*expected*])

The total number of hash entries in the CHT header for a ClipAV file does not match with the file's calculated number of hash entries.

Possible Cause

This error could be caused by incorrect CHT generation at authoring or by an AACS encryption problem.

Severity

This is a serious error indicating problems with the AACS encryption and is known to cause playability failures.

Possible Solution

This problem may be corrected by re-authoring or re-encrypting the image.

Related Rules

- **Incorrect CHT Size** will be triggered when the allocated size of the CHT does not match the size required for the CHT
- **Incorrect CHT Value** will be triggered when the hash calculation for a clip does not match the Content Hash Table

Type:	Blu-ray
Reference:	AACS Specifications Blue-ray Disc Pre-Recorded Book 0.912
Default Program Action:	Error

Rule ID: 885

Incorrect CHT Size

This Blu-ray error indicates that the content hash table size is not large enough to store the required hash table entries.

Background

For each physical layer of a BD-ROM, the Content Hash Table (CHT) is stored in the "\AACS" directory and in the "\AACS\DUPLICATE" directory. A single-layer disc has a single file named "ContentHash000.tbl", while a dual-layer disc has two files named "ContentHash000.tbl" for Layer 0 and "ContentHash001.tbl" for Layer 1. The Layer 0 and Layer 1 hash tables each need to be stored on the respective physical layer.

The CHT contains an 8-byte hash value for each hash unit of every Clip AV Stream file on the layer. The CHT file must contain adequate space to store these hash values. When this error is triggered, it indicates that the number of hash units reserved in the CHT is less than the number of hash units required to properly reflect the data in the image.

Possible Cause

This error is generally caused by the authoring system improperly calculating the number of hash units or hash digests required for a layer.

Severity

This is serious error indicating problems with the AACS protection. This error would be expected to cause playability failure or failure at AACS encryption/signing.

Additional Info

The Additional Info column in the analysis will identify the layer and whether the problem is with the main or duplicate CHT.

CHT L0 allocation size short. Image ([*UDF allocation size*]) required ([*required size*])

The allocation size specified by the UDF file system for the file \AACS\ContentHash000.tbl is too short.

CHT L0 DUP allocation size short. Image ([*UDF allocation size*]) required ([*required size*])

The allocation size specified by the UDF file system for the file \AACS\DUPLICATE\ContentHash000.tbl is too short.

CHT L1 allocation size short. Image ([*UDF allocation size*]) required ([*required size*])

The allocation size specified by the UDF file system for the file \AACS\ContentHash001.tbl is too short.

CHT L1 allocation size short. Image ([*UDF allocation size*]) required ([*required size*])

The allocation size specified by the UDF file system for the file \AACS\DUPLICATE\ContentHash001.tbl is too short.

Type:	Blu-ray
Reference:	AACS Specifications for BD Prerecorded Disc v0.912 2.3
Default Program Action:	Error

Rule ID: 886

Incorrect CHT Value

A value in the Content Hash Table does not match the recalculated value.

Background

The Blu-ray specifications require that certain files be protected by means of Content Hashing. On a Blu-ray video disc, the ClipAV files are divided into Hash Units, each consisting of 96 consecutive logical sectors. A hash value is then calculated on each Hash Unit and it is stored as an entry in the Content Hash Table.

During the analysis on BD images, these hash values are recalculated and compared to the hash value entries in the Content Hash Table. This rule is triggered if any of them do not match.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display one of the following messages with more specific information about the cause.

Layer [*LayerNo*] Image clip [*ClipNo*], Hash table values do not match

This message indicates that a recalculated hash value for a Hash Unit did not match with the hash value stored in the Content Hash Table for the same Hash Unit. The Hash Unit belongs to the ClipAV file identified by ClipNo. ClipNo is a 5-digit number used in the filename of ClipAV files (e.g. #####.m2ts).

LayerNo identifies the layer and content hash table file. On a single layer or layer 0 of a dual-layer image, the Content Hash Table filename is ContentHash000.tbl. On layer 1, the filename is ContentHash001.tbl. Files ContentHash000.tbl and ContentHash001.tbl are stored on layer 0 and layer 1 respectively.

Layer 0 Image clip [*ClipNo*], Hash table values do not match

This message indicates that a recalculated hash value for a Hash Unit did not match with the hash value stored in the Content Hash Table for the same Hash Unit. The Hash Unit belongs to the ClipAV file identified by ClipNo.ClipNo is a 5-digit number used in the filename of ClipAV files (e.g. #####.m2ts).

This message indicates that the error occurred on a ClipAV file stored on layer 0. This also identifies the error occurring in the file ContentHash000.tbl.

Layer 1 Image clip [*ClipNo*], Hash table values do not match

This message indicates that a recalculated hash value for a Hash Unit did not match with the hash value stored in the Content Hash Table for the same Hash Unit. The Hash Unit belongs to the ClipAV file identified by ClipNo.ClipNo is a 5-digit number used in the filename of ClipAV files (e.g. #####.m2ts).

This message indicates that the error occurred on a ClipAV file stored on layer 1. This also identifies the error occurring in the file ContentHash001.tbl.

Possible Cause

This problem has been seen when Content Hash Table files are corrupt due to physical defects on media, data corruption on hard disk images or corruption during network transfer of image. It also occurs when the Content Hash Table files are not created correctly. For example, this can occur if the hash entries are not recorded in the proper order.

Severity

This error is known to cause playability problems. Therefore, it should be considered an ERROR.

Solution

Since the Content Hash Table files are created during authoring, a solution may depend on whether or not the original image shows this problem. If the original image does not have this problem, then it indicates that the image got corrupt as it moved through the pre-mastering and mastering process (possible bad hard disk or network corruption). However, if the original source shows this error, then the problem may have been introduced during authoring.

If the problem occurs on a replica only, then it may be due to physical defects on the media.

Type:	MainChannel
Reference:	AACS Specifications for Blu-ray
Default Program Action:	Error

Rule ID: 859

Incorrect size for AACS Managed Copy Manifest file

The size for the AACS Managed Copy Manifest File (mcmf.xml) is more than the maximum allowed by the specifications.

Background

The Managed Copy Manifest file contains various data used for Managed Copy. Its file size must be less than or equal to 768KB.

Severity

If it is not the proper size, then the image will not be Managed Copy Compliant. Therefore, this condition is considered an ERROR.

Cause

This problem is typically caused by the authoring system.

Solution

A new image is required in order for the image to be Managed Copy Compliant. Contact the author or content owner for further assistance.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

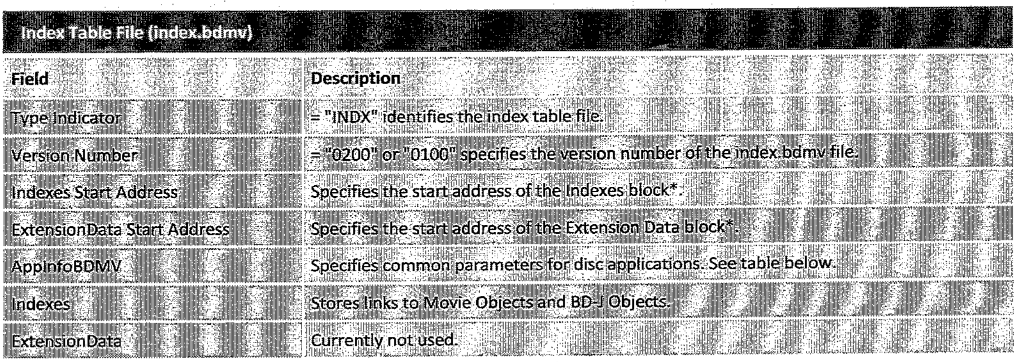
Rule ID: 1829

Index Table file 3D content flag not set

3D BD PlayList and/or SSIF file exists but the **SS_content_exists_flag** in the index.bdmv file is not set.

Background

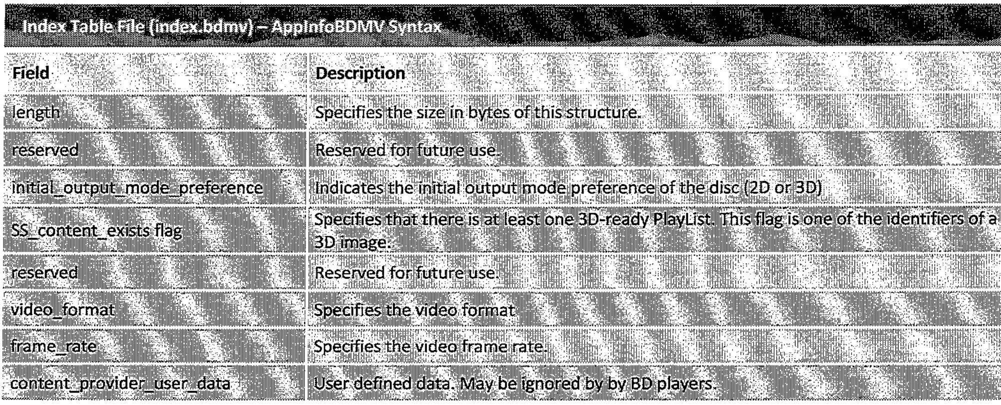
The AppInfoBDMV structure in the index table file (index.bdmv) includes the flag **SS_content_exists_flag** which specifies whether an image is 3D BD. When this flag is set, it indicates that there is at least one 3D-ready PlayList. The PlayList includes PlayItems which in turn have links to the Stereoscopic Interleaved files (SSIF).



Index Table File (index.bdmv)

Field	Description
Type Indicator	= "INDX" identifies the index table file.
Version Number	= "0200" or "0100" specifies the version number of the index.bdmv file.
Indexes Start Address	Specifies the start address of the Indexes block*.
ExtensionData Start Address	Specifies the start address of the Extension Data block*.
AppInfoBDMV	Specifies common parameters for disc applications. See table below.
Indexes	Stores links to Movie Objects and BD-J Objects.
ExtensionData	Currently not used.

* *Relative to the start of the index.bdmv file.*



Index Table File (index.bdmv) – AppInfoBDMV Syntax	
Field	**Description**
length	Specifies the size in bytes of this structure.
reserved	Reserved for future use.
initial_output_mode_preference	Indicates the initial output mode preference of the disc (2D or 3D)
SS_content_exists flag	Specifies that there is at least one 3D-ready PlayList. This flag is one of the identifiers of a 3D image.
reserved	Reserved for future use.
video_format	Specifies the video format.
frame_rate	Specifies the video frame rate.
content_provider_user_data	User defined data. May be ignored by by BD players.

This rule indicates that a 3D-ready PlayList was found and/or SSIF files were detected but the **SS_content_exists_flag** in the index table file is not set. This flag is the primary indicator that an image is 3D BD. If the flag is not set, then the image will be detected as a regular Blu-ray Video image and not as a 3D Blu-ray image.

Additional Info

When this rule is triggered, the **Additional Info** column in the analysis will display one of the following messages.

But 3D ready PlayList(s) detected

This condition indicates that a 3D-ready PlayList was found. If the author intended this image to be a 3D BD, then the SS_content_exists_flag must be set. Otherwise, the image may be considered as a normal Blu-ray Video.

But SSIF file(s) detected

This condition indicates that Stereoscopic Interleaved files were detected (.SSIF) but the SS_content_exists_flag is not set. If the author intended this image to be a 3D BD, then the SS_content_exists_flag must be set. Otherwise, the image may be considered as a normal Blu-ray Video.*

Severity

This condition is considered an ERROR since it will cause a 3D BD image to be detected as a normal Blu-ray Video image.

Cause

This problem is caused by the authoring system that created the image. If a 3D BD image was intended, then the **SS_content_exist_flag** must be set.

Solution

A new image is required. Contact Eclipse Support for further assistance.

Type: 3D-BD
Reference: 3D BD Specifications
Default Program Action: Error

Rule ID: 1723

ndex Table file 3D content flag set

The 3D Content Flag is set in the Index Table file (index.bdmv) but there are no Stereoscopic PlayLists, BD-J Application Profile 5 or Stereoscopic Output.

Background

The Index Table file includes a flag that specifies whether an image is 3D. However, any 3D image must ave at least one 3D-ready PlayList, a BD-J Application Profile 5 or Stereoscopic output. When this rule is triggered, it indicates that this flag is set but no 3D-ready PlayList, BD-J Application Profile 5 or stereoscopic output were found.

Severity

This condition is considered serious since the 3D flag indicates the image is 3D but does not meet all the equirements.

Cause

This problem is normally caused by the authoring system that created the image.

Solution

The image must be re-authored. Contact Eclipse Support for further assistance.

Type: Blu-ray
Reference: N/A
Default Program Action: Error

Rule ID: 1836

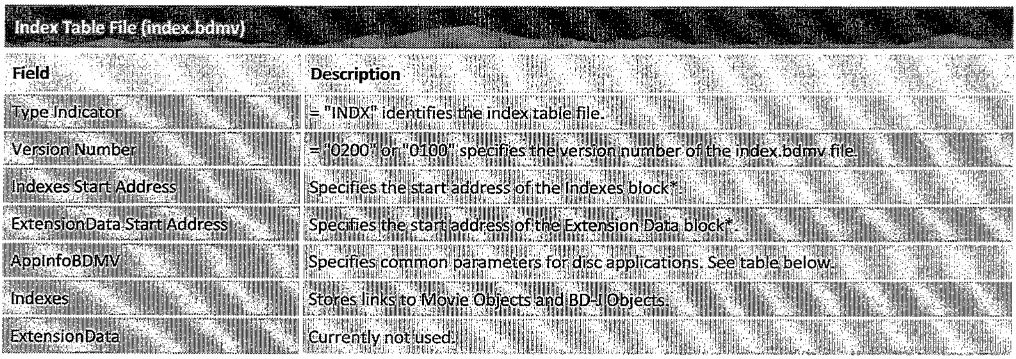
ndex Table file error

An error occurred when attempting to analyze the **Index.bdmv** file.

Background

The Index.bdmv file is the entry point into a Blu-ray image. It includes an index table that provides links to Movie Objects and BD-J Objects which define the navigation and playback content of the Blu-ray video. During analysis of a Blu-ray image, this file is loaded into memory and its contents are analyzed.

The contents of the index table file are as follows:



Index Table File (index.bdmv)

Field	Description
Type Indicator	= "INDX" identifies the index table file.
Version Number	= "0200" or "0100" specifies the version number of the index.bdmv file.
Indexes Start Address	Specifies the start address of the Indexes block*.
ExtensionData Start Address	Specifies the start address of the Extension Data block*.
AppInfoBDMV	Specifies common parameters for disc applications. See table below.
Indexes	Stores links to Movie Objects and BD-J Objects.
ExtensionData	Currently not used.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will identify the condition that triggered the rule with one of the following messages:

Failed to load \BDMV\index.bdmv

This condition indicates that the EclipseSuite tools were unable to load this file for analysis. Therefore, it is considered an ERROR.

This is a general error condition which may be triggered by anything that anything that prevents loading of the index.bdmv file. This may include file read errors or not enough system resources.

Invalid type_indicator field in \BDMV\index.bdmv

The type_indicator field of the index.bdmv file identifies the file as the Blu-ray Index file. This field must be set to "INDX".

This condition is typically caused by the authoring system not setting the type_indicator to the correct value. However, it is possible that file corruption may also trigger this condition.

Invalid version_number field in \BDMV\index.bdmv

The version number field of the index table file is invalid. The specifications require it to be set to "0200" or "0100".

Severity

The three conditions above that trigger this rule are considered serious and, therefore, this rule is considered an ERROR.

Cause

The possible cause of this rule depends on the condition that triggered it:

1. **Failed to load \BDMV\index.bdmv** - This normally indicates physical corruption on media or a corrupt file. It may also indicate that your computer system may not have enough resources to load this file into memory for analysis.
2. **Invalid type_indicator field in \BDMV\index.bdmv** - This condition is typically caused by the authoring system that created the image.
3. **Invalid version number field in \BDMV\index.bdmv** - This condition is typically caused by the

authoring system that created the image.

Solution

A new image is required. Contact Eclipse Support for further assistance.

Type:	Blu-ray
Reference:	3D BD Specifications
Default Program Action:	Error

Rule ID: 1722

Invalid BDCMF AACS attribute

This error occurs when the AACS attribute for the CPS element contains an invalid value. It should contain either 'USE' or 'NONE'.

Background

The BDCMF.CMF file includes the CPS element which is used to specify whether or not an image is protected with AACS and/or BD+. The CPS element is formatted as follows:

```
<CPS AACS="USE" BDP="NONE"/>
```

If the image is protected with AACS, then the AACS attribute must be set to "USE". The only other valid value is "NONE" which indicates that the image is not protected with AACS. This error indicates that a different value was found. When this rule is triggered, the Additional Info column in the Analysis tab will display the value that was found.

Type:	Blu-ray
Reference:	BDCMF Specifications Version 0.90 3.1.1.5 pg. 11
Default Program Action:	Error

Rule ID: 894

Invalid BDCMF BDPlus attribute

The BDCMF.CMF file contains an invalid value for the BDP element.

Background

The BDP (BD+) refers to an enhanced copy protection that can be applied to a Blu-ray image.

BDP is a mandatory element contained within the Content Protection System (CPS) section of the BDCMF.CMF file. The BDP element must be set to either "USE" which means this copy protection is applied to the media or "NONE" which means the copy protection will not be applied.

<u>**Example:**</u>

```
<General>
    <CMFVersion>BDCMF 0.90</CMFVersion>
    <MasterID>BDCMF A-0605-0001</MasterID>
    <Date Created="2006-02-20T21:00:00." LastRevised="2006-02-20T21:00:00."/>
    <CPS AACS="USE" BDP="NONE"/>
    <CMFType>A</CMFType>
    <Note>Add bonus track</Note>
</General>
```

Possible Cause

An incorrect value was placed in the BDCMF.CMF file during creation.

Severity

This rule is considered an error since it may be impossible for a pre-mastering or mastering system to process this image.

Possible Solution

Since the reference information to this file is almost always the same, it is possible to correct it by manually editing the BDCMF.CMF file. The reference can also be copied from a known good file. However, you must be familiar with the CMF specifications and know where the changes need to be made.

If editing is not possible, then the image must be recreated.

Type:	Blu-ray
Reference:	BDCMF Specification Version 0.90 Section 3.1.1.5 Pg 11
Default Program Action:	Error

Rule ID: 895

Invalid BDCMF BDType attribute

The BDCMF.CMF file contains an invalid BDType attribute.

Background

In the BDCMF specification, the BDType attribute describes whether the image is a "BD" or "BD9". BD refers to 25GB or 50GB Blu-ray image. BD9 is a proposed BD format that specifies a 9 GB High Definition red laser disc, which is compatible with DVD manufacturing lines.

Additional Info

When this rule is triggered, the **Additional Info** column in analysis will display the value that was found.

Example:

```
<DiscInfo>
    <DiscType GeneralType="BD-ROM" BDType="BD" HybridType="NOHYBRID" DiscSize="12cm" />
    <LayerInfo Total="2" BD="2" L0SectorSize="4148224" />
    <BDInfo Density="25G" />
    <Note>This is a regular dual layer disc</Note>
</DiscInfo>
```

Error Severity

The BDType attribute must be specified in order to identify the type of image being processed. Therefore, this is considered an error.

Possible Cause

This problem typically occurs when the image is authored or if it is edited after authoring.

Possible Solution

If the correct BDType is known, it is possible to correct it by manually editing the BDCMF.CMF file. The BDType can also be copied from a known good file. However, you must be familiar with the CMF specifications and know where the changes need to be made.

If editing is not possible, then the image must be re-authored.

Type:	Blu-ray
Reference:	BDCMF V.0.90, 3.1.2.1
Default Program Action:	Error

Rule ID: 897

Invalid BDCMF CPS Unit number

The BDCMF file has an invalid CPS Unit Number of a ClipAV file.

Background

The CPS Unit Number specifies the encryption key to use for encrypting a ClipAV file. On a BDCMF image, each ClipAV file is referenced in the BDCMF.CMF file. Each ClipAV entry in this file includes the attribute CPSUnitNo. This is a mandatory attribute and must be set to an integer value. Currently only one CPS Unit is used for encryption of BD images. Therefore, it is expected that the CPSUnitNo be set to a value of '1'. However, in the future, more than one CPSUnits may be defined. In such case, the XML element NumOfCPSUnit is used to specify the total number of CPS Units available.

This message indicates that the CPSUnitNo value is less than '1' or greater than the value specified by NumOfCPSUnit.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display one of the following messages indicating the exact cause of this error.

Clip [*ClipAV file*] CPSUnitNo [*CPSUnitNo*]

This message indicates that the CPSUnitNo for the ClipAV file is greater than the total number of CPS Units specified by NumOfCPSUnit or it is less than 1. Currently only one CPS Unit is used for encryption. Therefore, it is expected that the CPSUnitNo be set to '1'.

Clip [*ClipAV file*] missing CPSUnitNo

This message indicates that there is no value specified for the CPSUnitNo for the ClipAV file. Currently only one CPS Unit is used for encryption. Therefore, it is expected that the CPSUnitNo be set to '1'.

Clip missing CPSUnitNo

This message indicates that the XML element CPSUnitNo is missing from a ClipAV file.

Severity

This rule is considered an ERROR since it may cause the AACS processing of an image to abort.

Cause

This problem is typically caused by the utility that created the image.

Solution

It may be possible to correct this problem by manually editing the BDCMF file. However, you must be familiar with the BDCMF specifications in order to make the necessary changes. Contact Eclipse Customer Support for further assistance.

If editing is not possible, then the image must be re-authored.

Type:	Blu-ray
Reference:	BDCMF Specifications
Default Program Action:	Error

Rule ID: 1410

Invalid BDCMF Density attribute

The Density XML attribute for the \DISCINFO\BDINFO element is invalid.

Background

The BDCMF.CMF file must specify the density, or capacity, of the BD image. This is done via the Density attribute for the BDInfo XML element, as shown in the XML fragment below:

```
...
<DiscInfo>
    <DiscType GeneralType="BD-ROM" BDType="BD" HybridType="NOHYBRID" DiscSize="12cm" />
    <LayerInfo Total="2" BD="2" L0SectorSize="4148224" />
    <BDInfo Density="25G" />
    <Note>This is a regular dual layer disc</Note>
</DiscInfo>
...
```

The **Density** attribute must specify a density of 25GB or 50GB. Any other value is invalid (27GB and 54GB are reserved for future use).

Additional Info

When this rule is triggered, the **Additional Info** column in the analysis will display the Density that was found.

Severity

This rule was initially recommended by the Blu-ray format creators to be set to an ERROR severity. However, this rule is only reporting the Density value that was found in the BDCMF.CMF file. On a disc, the density value will be taken from the PIC data.

Cause

This problem is caused by the utility that created the image.

Solution

Since the BDCMF.CMF file is a text file, this problem can be corrected easily if the correct value is known and if you are familiar with the structure of this file. If you are not familiar with the structure of this file or you do not know the correct value, then this image must be returned to authoring.

If you proceed to edit the BDCMF.CMF file, it is recommended that you make a backup copy before editing.

Contact Eclipse Customer Support for further assistance.

Eclipse Customer Support
Phone: (925) 598-0300
Email: Support@eclipsedata.com

Type: Blu-ray
Reference: BDCMF Specifications
Default Program Action: Error

Rule ID: 1404

Invalid BDCMF DiscSize attribute

The DiscType element contains an invalid DiscSize attribute.

Background

DiscSize is a mandatory attribute of the DiscType element. It describes the diameter of the physical disc in centimeters. Valid DiscSize values are "12cm" for standard size or "8cm" for small BD discs.

Example:

```
...
<DiscInfo>
    <DiscType GeneralType="BD-ROM" BDType="BD" HybridType="NOHYBRID" DiscSize="12cm" />
    <LayerInfo Total="2" BD="2" L0SectorSize="4148224" />
    <BDInfo Density="25G" />
    <Note>This is a regular dual layer disc</Note>
</DiscInfo>
...
```

Possible Cause

This condition typically occurs when the image is created.

Severity

This rule is considered an error since it is not possible to process the image with this missing attribute.

Possible Solution

The image must be re-created.

Type: Blu-ray
Reference: BDCMF V.0.90 sect. 3.1.2.1
Default Program Action: Error

Rule ID: 1400

Invalid BDCMF GeneralType attribute

The GeneralType attribute contains an invalid value.

Background

GeneralType is a required attribute for the DiscType element. It is used to identify the disc type. Currently, the only valid value for GeneralType is "BD-ROM".

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis tab will display the value found.

Example:

```
...
<DiscInfo>
     <DiscType GeneralType="BD-ROM" BDType="BD" HybridType="NOHYBRID" DiscSize="12cm" />
     <LayerInfo Total="2" BD="2" L0SectorSize="4148224" />
     <BDInfo Density="25G" />
     <Note>This is a regular dual layer disc</Note>
</DiscInfo>
...
```

Possible Cause

This is typically cause during authoring of the image or if edited after authoring.

Severity

This rule is considered an error since it may not be possible to process the image with an invalid value.

Possible Solution

Since "BD-ROM" is currently the only value used, it is possible to correct it by manually editing the BDCMF.CMF file. The reference can also be copied from a known good file. However, you must be familiar with the CMF specifications and know where the changes need to be made.

If editing is not possible, then the image must be re-authored.

Type: Blu-ray
Reference: BDCMF Specs V0.90 sec.3.1.2.1
Default Program Action: Error

Rule ID: 896

Invalid BDCMF HybridType attribute

The HybridType attribute of the DiscType element contains an invalid value.

Background

HybridType is a required attribute for the DiscType element and describes whether a BD image also contains a CD or DVD layer. The valid values for HybridType are "NOHYBRID","CD RO" or "DVD RO". "NOHYBRID" describes a BD disc with no CD or DVD layer. "CD RO" describes a BD and CD hybrid disc. "DVD RO" describes a BD and DVD hybrid disc. See the Additional Information section of the Analysis tab for the invalid value found. See the BDCMF example below.

Example:

```
...
<DiscInfo>
    <DiscType GeneralType="BD-ROM" BDType="BD" HybridType="NOHYBRID" DiscSize="12cm" />
    <LayerInfo Total="2" BD="2" L0SectorSize="4148224" />
    <BDInfo Density="25G" />
    <Note>This is a regular dual layer disc</Note>
</DiscInfo>
...
```

Possible Cause

An incorrect value was specified in the BDCMF.CMF file during the image creation.

Severity

This rule is considered an error since it is not possible to process the image with an invalid value.

Possible Solution

Since the hybrid type value should be known, it is possible to correct it by manually editing the BDCMF.CMF file. The value can also be copied from a known good file. However, you must be familiar with the CMF specifications and know where the changes need to be made.

If editing is not possible, then the image must be re-created.

Type:	Blu-ray
Reference:	BDCMF Specs V0.90 sec.3.1.2.1
Default Program Action:	Error

Rule ID: 898

Invalid BDCMF LayerInfo BD attribute

The BD attribute of the LayerInfo element contains an invalid value.

Background

The BDCMF LayerInfo BD attribute is required and describes the total number of BD layers on the disc. Currently, the valid values for this attribute are "1" or "2". See the additional info section of the Analysis tab for the invalid value found. See the BDCMF.CMF example below.

Example:

```
...
<DiscInfo>
    <DiscType GeneralType="BD-ROM" BDType="BD" HybridType="NOHYBRID" DiscSize="12cm" />
    <LayerInfo Total="2" BD="2" L0SectorSize="4148224" />
    <BDInfo Density="25G" />
    <Note>This is a regular dual layer disc</Note>
</DiscInfo>
...
```

Possible Cause

This condition typically occurs when the image is created.

Severity

This rule is considered an error since it is not possible to process the image with an invalid value.

Possible Solution

Since the attribute value is generally known, it is possible to correct it by manually editing the BDCMF.CMF file. The value can also be copied from a known good file. However, you must be familiar with the CMF specifications and know where the changes need to be made.

If editing is not possible, then the image must be recreated.

Type:	Blu-ray
Reference:	BDCMF Specs V0.90 sec.3.1.2.1
Default Program Action:	Error

Rule ID: 1402

Invalid BDCMF LayerInfo Total attribute

The Total attribute for the LayerInfo element has an invalid value.

Background

Total is a required attribute for the LayerInfo element that describes the total number of layers on a BD image. Currently, the valid values for this attribute are "1", "2", or "3". See the additional info section of the Analysis tab for the invalid value found. See the BDCMF.CMF example below.

```
...
<DiscInfo>
    <DiscType GeneralType="BD-ROM" BDType="BD" HybridType="NOHYBRID" DiscSize="12cm" />
    <LayerInfo Total="2" BD="2" L0SectorSize="4148224" />
    <BDInfo Density="25G" />
    <Note>This is a regular dual layer disc</Note>
</DiscInfo>
...
```

Possible Cause

An incorrect value was specified in the BDCMF.CMF file during the image creation.

Severity

This rule is considered an error since it is not possible to process the image with an invalid value.

Possible Solution

Since the value for the Total attribute should be known, it is possible to correct it by manually editing the BDCMF.CMF file. The value can also be copied from a known good file. However, you must be familiar with the CMF specifications and know where the changes need to be made.

If editing is not possible, then the image must be re-created.

Type:	Blu-ray
Reference:	BDCMF Specs V0.90 sec.3.1.2.1
Default Program Action:	Error

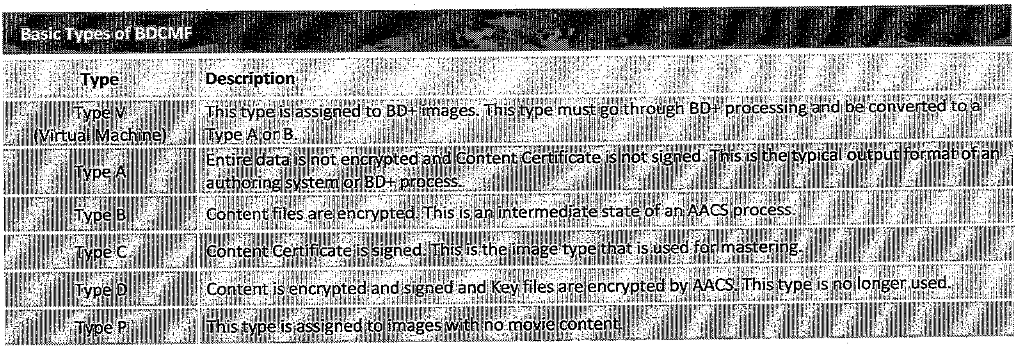
Rule ID: 1401

Invalid BDCMF Type Element

The BDCMF image does not have a valid CMFType element describing it as a Type A, B, C or D image.

Background

The CMFType XML element is used to describe an image's current process status. It is used to indicate the image's status through the encryption and signing process. Below are the valid CMFType values.



Basic Types of BDCMF

Type	Description
Type V (Virtual Machine)	This type is assigned to BD+ images. This type must go through BD+ processing and be converted to a Type A or B.
Type A	Entire data is not encrypted and Content Certificate is not signed. This is the typical output format of an authoring system or BD+ process.
Type B	Content files are encrypted. This is an intermediate state of an AACS process.
Type C	Content Certificate is signed. This is the image type that is used for mastering.
Type D	Content is encrypted and signed and Key files are encrypted by AACS. This type is no longer used.
Type P	This type is assigned to images with no movie content.

Additional Info

When this rule is triggered, the Additional Info column in the Analysis will display the value that was found for the CMFType.

Severity

This rule is considered an error since the CMFType specifies the encryption status of an image. Without the proper CMFType value, it may be impossible to know what the next step in the AACS process is for this image.

Cause

This problem is caused by the authoring system that created the image. However, during the different steps of the AACS process, other utilities will have to update the CMFType. It is also possible that these utilities may fail update this element with the correct value.

Solution

Since the BDCMF.CMF file is a text file, this problem can be corrected easily if the correct value is known and if you are familiar with the structure of this file. If you are not familiar with the structure of this file or you do not know the correct value, then processing of this image may not be possible.

If you proceed to edit the BDCMF.CMF file, it is recommended that you make a backup copy before editing.

Contact Eclipse Customer Support for further assistance.
Eclipse Customer Support
Phone: (925) 598-0300
Email: Support@eclipsedata.com

Type:	Blu-ray
Reference:	BDCMF Specifications
Default Program Action:	Error

Rule ID: 892

Invalid CPS Unit number

The CPS Unit number assigned to a Title, First Playback or Top Menu is invalid.

Background

All Titles, including First Playback and Top Menu must be assigned to a CPS Unit. All CPS Units are numbered sequentially starting at 1.

The Index table file (index.bdmv) includes a list of all Titles, including the First Playback and Top Menu. For each, the index table file specifies an ID, an object type (Movie Object or BD-J Object), filename and total number of Titles specified in the index table.

Similarly, the Unit Key file (Unit_Key_RO.inf) includes a header that contains a list of Titles, including First Playback and Top Menu. For each, the Unit Key file specifies the same ID as the index table file. It includes the CPS Unit number that is assigned to each Title.

Since both Index Table and Unit Key files should include the same references to First Playback, Top Menu and other Titles, the EclipseSuite tools analyze the contents of both files for any inconsistencies. This rule is triggered when a Title, in the Unit Key file, is assigned an invalid CPS Unit number value.

Additional Info

This rule is caused by one of the following conditions as displayed in the Additional Info column in Analysis.

'CPS_Unit_number' for First Playback ([*CPSUnit#*]) > 'Num_of_CPS_Unit' ([*TotalNoOfCPSUnits*])

The CPS Unit number value for the First Playback is greater than the total number of CPS Units recorded on the disc.

The CPS Unit Key file includes a field that specifies the total number of CPS Units recorded on the disc. Since the CPS Units are numbered sequentially starting at 1, any CPS Unit number value should never be greater than the total number of CPS Units.

FirstPlayback Title, Movie Object ([*MovObj#*]) has no CPS Unit value assigned

The First Playback is recorded and it is a Movie Object. However it has no CPS Unit value assigned (i.e. CPS Unit number = 0). If a First Playback is recorded, it must be assigned a CPS Unit value starting from 1.

FirstPlayback Title, BD-J Object '[*BDJObj#*].bdjo' has no CPS Unit value assigned

The First Playback is recorded and it is a BD-J Object. However it has no CPS Unit value assigned (i.e. CPS Unit number = 0). If a First Playback is recorded, it must be assigned a CPS Unit value starting from 1.

FirstPlayback Title has no CPS Unit value assigned

The First Playback is recorded but the EclipseSuite tools were unable to determine if it is a Movie Object or BD-J Object. Regardless of the type, it has no CPS Unit value assigned (i.e. CPS Unit number = 0). If a First Playback is recorded, it must be assigned a CPS Unit value starting from 1.

'CPS_Unit_number' for Top Menu ([*TopMenu#*]) > 'Num_of_CPS_Unit' ([*TotalNoOfCPSUnits*])

The CPS Unit number value for the Top Menu is greater than the total number of CPS Units recorded on the disc.

The CPS Unit Key file includes a field that specifies the total number of CPS Units recorded on the disc. Since the CPS Units are numbered sequentially starting at 1, any CPS Unit number value should never be greater than the total number of CPS Units.

TopMenu Title, Movie Object ([*MovObj#*]) has no CPS Unit value assigned

The Top Menu is recorded and it is a Movie Object. However it has no CPS Unit value assigned (i.e. CPS Unit number = 0). If a Top Menu is recorded, it must be assigned a CPS Unit value starting from 1.

TopMenu Title, BD-J Object '[*BDJObj#*].bdjo' has no CPS Unit value assigned

The Top Menu is recorded and it is a BD-J Object. However it has no CPS Unit value assigned (i.e. CPS Unit number = 0). If a Top Menu is recorded, it must be assigned a CPS Unit value starting from 1.

TopMenu Title has no CPS Unit value assigned

The Top Menu is recorded but the EclipseSuite tools were unable to determine if it is a Movie Object or BD-J Object. Regardless of the type, it has no CPS Unit value assigned (i.e. CPS Unit number = 0). If a Top Menu is recorded, it must be assigned a CPS Unit value starting from 1.

'CPS_Unit_number' for Title [*Title#*] ([*CPSUnit#*]) > 'Num_of_CPS_Unit' ([*NumOfCPSUnits*])

The CPS Unit number value for the Title# is greater than the total number of CPS Units recorded on the disc.

The CPS Unit Key file includes a field that specifies the total number of CPS Units recorded on the disc. Since the CPS Units are numbered sequentially starting at 1, any CPS Unit number value should never be greater than the total number of CPS Units.

Title ([*Title#*]), Movie Object ([*MovObj#*]) has no CPS Unit value assigned

Title# is recorded and it is a Movie Object. However it has no CPS Unit value assigned (i.e. CPS Unit number = 0). If a Title is recorded, it must be assigned a CPS Unit value starting from 1.

Title ([*Title#*]), BD-J Object '[*BDJObj#*].bdjo' has no CPS Unit value assigned

Title# is recorded and it is a BD-J Object. However it has no CPS Unit value assigned (i.e. CPS Unit number = 0). If a Title is recorded, it must be assigned a CPS Unit value starting from 1.

Title ([*Title#*]) has no CPS Unit value assigned

Title# is recorded but the EclipseSuite tools were unable to determine if it is a Movie Object or BD-J Object. Regardless of the type, it has no CPS Unit value assigned (i.e. CPS Unit number = 0). If a Title is recorded, it must be assigned a CPS Unit value starting from 1.

Severity

The conditions listed above are considered an ERROR since it is possible that they may lead to playability problems.

Cause

This problem is caused by the authoring application that created the image.

Solution

The image must be authored. Consult with the customer or company that authored the image. Contact Eclipse Support for further assistance.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

Rule ID: 1871

Invalid entry in Managed Copy Manifest

The Managed Copy Manifest file contains an invalid entry.

Background

Some movie studios require specific settings in the Managed Copy Manifest file (mcmf.xml). This rule indicates that certain entry values are not valid for the movie studio of the image.

Example of a Managed Copy Manifest File:

```
<?xml version="1.0" encoding="UTF-8"?>
<mcmfManifest xmlns="http://www.aacsla.com/2006/02/bdmcManifest"
contentID="0x00000000000000000000000000000001">
  <URIList>
    <URI>http://example.com/ManagedCopy/00000001/</URI>
    <URI>http://example.net/ManagedCopy/00000001/</URI>
  </URIList>
  <MCUALL>
    <DirectoryName>BDMV</DirectoryName>
  </MCUALL>
  <MCUPARTIAL ID="0x0001">
    <FileName>BDMV/PLAYLIST/00000.mpls</FileName>
    <FileName>BDMV/CLIPINF/00000.clpi</FileName>
    <FileName>BDMV/STREAM/00000.m2ts</FileName>
    <FileName>BDMV/BDJO/00000.bdjo</FileName>
    <FileName>BDMV/JAR/00000.jar</FileName>
    <FileName dest="BDMV/index.bdmv">PARTIALDB/index.bdmv</FileName>
    <FileName dest="BDMV/MovieObject.bdmv">PARTIALDB/MovieObject.bdmv</FileName>
    <description lang="eng" text="Lion" />
    <description lang="deu" text="Löwe" />
  </MCUPARTIAL>
</mcmfManifest>
```

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display more details with one of the following messages.

MCUALL element present

This condition indicates that the XML element 'MCUALL' *is invalid for the movie studio of the image being analyzed.*

MCUPARTIAL element present

This condition indicates that the XML element 'MCUPARTIAL' *is invalid for the movie studio of the image being analyzed.*

URI element invalid, expected '[*ExpectedURI*]' actual '[*ActualURI*]'

This condition indicates that the XML element 'URIList' *contains an invalid URI for the movie studio of the image being analyzed.*

Severity

This rule is related to the Title Structure analysis. This error indicates that the image being analyzed did not conform to the title structure requirements. Therefore, this condition is considered an ERROR.

Cause

This condition is normally caused during authoring of the image.

Solution

This error does not indicate any problem with the Blu-ray format. It is an error that gets triggered when the layout of the image does not conform to a predefined layout specified by the movie studio. Check with the authoring or movie studio whether it is ok to continue with the image or whether the image should be re-authored.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

Rule ID: 1718

Invalid ISAN Number

The International Standard Audiovisual Number (ISAN) is invalid.

Background

The ISAN number is used in images that are Managed Copy ready. The ISAN number is part of the Content ID field of the Managed Copy Manifest File (\AACS\mcmf.xml). This error indicates that the Content ID value is not in the proper format or that it contains invalid information.

The Content ID field is a 128-bit value, which includes the ISAN number and has the following structure:

Content ID Type: 4 bits
Reserved: 28 bits
ISAN number: 96 bits

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display more details with one of the following messages.

Content ID Invalid: *[## ## ## ## ## ## ## ## ## ## ## ## ## ## ## ##]*

The Content ID bits are invalid.

In this case, this condition indicates that the first four bytes consisting of the Content ID and Reserved bits are invalid. They should have the value:

80h 00h 00h 00h

The value of the Content ID and Reserved fields is set during the authoring process of the image.

Could not calculate ISAN check digits: *[## ## ## ## ## ## ## ## ## ## ## ## ## ## ## ##]*

This condition occurs when the EclipseSuite tools are unable to validate the ISAN number.

The ISAN number includes a check-digit which can be used to verify if the other numbers are correct. This may indicate an internal program error or invalid characters in the ISAN number.

Content ID ISAN Invalid: [*## ## ## ## ## ## ## ## ## ## ## ##*]

This message indicates that the ISAN number in bytes 4-16 contain an invalid value. This message will display the actual value found. However, note that the current version of the specifications allow the ISAN value to be all zeroes. Therefore, if the value displayed by this message is all zeroes, then this warning can be ignored.

Severity

If the ISAN number is all zeroes, then this rule can be ignored since it is allowed by current specifications. Otherwise, it may be a problem and it is the reason this condition is a WARNING.

Cause

This problem is caused by the authoring application that created the image.

Solution

If the ISAN is all zeroes then ignore this rule. If it is non-zero, check with the author/owner of the image to verify the severity of this rule. There may be cases in which this condition may be a problem and others in which it may not. Only the author/owner can determine the severity.

Type:	Blu-ray
Reference:	AACS Specifications

Introduction and Common Cryptographic Elements Book

Default Program Action: Warning

Rule ID: 1586

Invalid Navigation command

A Navigation Command did not include enough parameters (operands) or it included too many.

Background

The Blu-ray specifications Navigation commands have 0, 1 or 2 operands. Each Navigation Command includes an Operation Code, which identifies the type of command and 0, 1 or 2 Operands, which identify a Source and Destination.

This rule is triggered when a Command such as a Branch Command (e.g. GoTo, Jump or Play) does not have the correct number of Operands.

The **Navigation Command** structure is as follows.

b95 . . . . b64	b63 . . . . b32	b31 . . . . b0
Operation Code	Operand (Destination)	Operand (Source)

The **Operation Code** format is as follows.

b95	b94	b93	b92	b91	b90	b89	b88
Operand Count			Command Group		Command Sub-Group		
b87	b86	b85	b84	b83	b82	b81	b80
I_flag for Operand 1	I_flag for Operand 2	Reserved		Branch Option			
b79	b78	b77	b76	b75	b74	b73	b72
Reserved				Compare Option			
b71	b70	b69	b68	b67	b66	b65	b64
Reserved			Set Option				

The **Operand format** is as follows when the I_flag for this Operand is 1b.

bn + 31	bn + 30	bn + 29	bn + 28	bn + 27	bn + 26	bn + 25	bn + 24
REG_flag	Reserved						

bn + 23	bn + 22	bn + 21	bn + 20	bn + 19	bn + 18	bn + 17	bn + 16
Reserved							

bn + 15	bn + 14	bn + 13	bn + 12	bn + 11	bn + 10	bn + 9	bn + 8
Reserved				Register Number (b11 - b8)			

bn + 7	bn + 6	bn + 5	bn + 4	bn + 3	bn + 2	bn + 1	bn
Register Number (b7 - b0)							

Additional Info

When this rule is triggered, the Additional Info column in the Analysis will display one of the following messages describing the cause of this warning.

Blu-ray Video: [*Command-SubGroup*] operand count should be 1 instead of ([*OperandCount*])

The number of Operands for the following commands should be 1.
GoTo-Goto - Only the Destination operand must be specified.
Jump-JumpObject - Only the Destination operand must be specified.
Jump-CallObject - Only the Destination operand must be specified.
Play-PlayList - Only the Destination operand must be specified.

Blu-ray Video: [*Command-SubGroup*] operand count should be 2 instead of ([*OperandCount*])

The number of operands for the following commands should be 2.

PlayList-PlayItem - Both Source and Destination operands must be specified.
Play-PlayListMark - Both Source and Destination operands must be specified.

Blu-ray Video: First Operand is for PSR ([*Value*])

When the REG_flag bit in the first Operand is 0b, bits 0 thru 11 specify up to 128 Player Status Registers (PSR). The value of these bits must be between 0 and 127.

Blu-ray Video: Second Operand is for PSR ([*Value*])

When the REG_flag bit in the second Operand is 0b, bits 0 thru 11 specify up to 128 Player Status Registers (PSR). The value of these bits must be between 0 and 127.

Severity

This rule is only considered a WARNING since it is unknown as to how it may affect playability.

Cause

This problem is caused by the authoring system that created the image.

Solution

This problem cannot be corrected in pre-mastering or mastering. The image must be re-authored.

Type:	Blu-ray
Reference:	Blu-ray Disc Read Only Format Part 3: Audio Visual Basic Specifications (3-1 Core Specifications)Section 10.4: Navigation Commands
Default Program Action:	Warning

Rule ID: 852

Invalid or missing BDCMF schema field

The schema attribute in the BDCMF.CMF file is missing or has an invalid value.

Background

The BDCMF.CMF file is formatted in XML and requires a schema to be specified. The schema is used to define the rules that help in interpreting the contents of an XML file.

Example:

```
<?xml version="1.0" encoding="UTF-8"?>
<CMFInfo xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="BDCMF schema .xsd">
```

Additional Info

When this error occurs, the **Additional Info** column in the analysis will display the expected value with the following message.

Expected: `(XSI:NONAMESPACESCHEMALOCATION="BDCMF SCHEMA .XSD")`

Error Severity

This rule is considered an error since the schema is used to interpret the contents of the BDCMF.CMF file. Although this is a requirement of the BDCMF specifications, currently it does not cause a problem with the Eclipse process. However, if you are using other utilities or systems to process this image, it is unknown whether this will cause a problem.

Possible Cause

This problem is caused by the utility that created the BDCMF.CMF file.

Possible Solution

Since the schema is set to a fixed value regardless of image type, it is possible that it can be corrected by manually editing the BDCMF.CMF file. However, make sure that you are familiar with the XML format before making any changes.

If editing is not possible, then the file must be re-created.

Type:	Blu-ray
Reference:	BDCMF Specifications v0.90
Default Program Action:	Error

Rule ID: 888

Invalid or missing BDCMF version field

The required BDCMF Version element is missing or contains an invalid value.

Background

The BDCMF Version field describes the version to which the BDCMF image conforms. The current valid value is "BDCMF 0.90". This value may increment to conform to future BDCMF specification revisions. When this rule is triggered, the **Additional Information** column in the Analysis tab will display the value found.

Example:

```
<General>
   <CMFVersion>BDCMF 0.90</CMFVersion>
   <MasterID>BDCMF A-0605-0001</MasterID>
   <Date Created="2006-02-20T21:00:00." LastRevised="2006-02-20T21:00:00."/>
   <CPS AACS="USE" BDP="NONE"/>
   <CMFType>C</CMFType>
   <Note>Add bonus track</Note>
</General>
```

Possible Cause

This problem occurs when the image is authored or if it is edited after authoring.

Severity

This rule is considered an error since it may not be possible to process the image with an invalid value.

Possible Solution

If the correct BDCMF version is known, it is possible to correct it by manually editing the BDCMF.CMF file. The reference can also be copied from a known good file. However, you must be familiar with the CMF specifications and know where the changes need to be made.

If editing is not possible, then the image must be re-authored.

Type:	Blu-ray
Reference:	BDCMF Specs V0.90 sec 3.1.1.1
Default Program Action:	Error

Rule ID: 889

Invalid UTC-8 octet sequence

One of the XML image files contains an illegal character.

Background

XML documents include a field that specifies the encoding used by the document (i.e. file). Different encodings are used to specify different character sets required by different languages. The most common (and default for all XML image files) is UTF8. If an authoring application inserts a character that is not covered by UTF8, then this rule is triggered. This condition typically occurs when characters from other encodings (character sets) are used in a document formatted with UTF8. This will occur mostly in informational user defined fields such as `<TitleInfo>` element of the BDCMF.CMF file. This element contains Title and Copyright information of the Blu-ray Video and it is in these types of user-defined fields where this error would be expected.

Severity

This condition is considered an ERROR since it affects processing of the file.

Cause

This condition is typically caused by the authoring application that created the image. However, it is also possible that any other utility that edits the file may introduce characters that are not supported by the current encoding of the file.

Solution

Since this condition is normally caused by a character in one of the user-defined fields in a file, it is often easy to correct by manually editing the file and removing the offending character. However, care should be taken when editing these files. Any mistake may result in worse condition. Always make a backup copy before editing. If you are not familiar with the format of this file or if you do not want to manually edit the file, contact the author of this image or Eclipse Support for further assistance. Otherwise, you may need to request a new image.

WARNING! If you are not familiar with the format of the file, DO NOT edit the manual and contact Eclipse Support for further assistance.

Type:	Other
Reference:	XML Specifications
Default Program Action:	Error

Rule ID: 1778

JAR Manifest File analysis error

This is a general error message that is triggered when analyzing the JAR Manifest file. For the specific cause of this error, please check the message in the Additional Info column in the Analysis. The possible causes of this error are listed and described in the **Additional Info** section.

Background

A JAR File includes a single Manifest file which contains a list of all the files in the JAR File (excluding the Manifest file itself) and a message digest for each. The JAR Manifest File is stored in the directory META-INF inside the JAR File. The Manifest file includes a main section followed by a list of entries for each file inside the JAR file. Each file entry includes a filename and a SHA1-Digest for the file. An entry must exist for each signed file inside the JAR File.

Manifest File Syntax	
Manifest-Version:	These are all possible attributes in the main section of the Manifest file. For a complete list, refer to the JAR File Specifications.
Created By:	
Signature Version:	Below the main section is a list of entries; one for each signed file inside the JAR File.
Class Path:	
File Entries	The remaining sections are each an entry that identifies a file inside the JAR file. Each entry includes the following fields.
Name:	This is a relative path to a file inside the JAR file.
SHA1-Digest:	This is a SHA-1 digest value calculated over the file data.

Example:

```
Manifest-Version: 1.0

Name: a.class
SHA1-Digest: 4iajlE8csRjGe2GRG4CWgKJ3?Xc=

Name: b.class
SHA1-Digest: TGeoPF5MlN1FVrwE4BiRLipo4QB=
...
```

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display more details with one of the following messages.

Reference:

- ***JARFile*** specifies the JAR filename that is being analyzed.
- ***ManifestFile*** specifies the Manifest file inside the JAR file that is being analyzed.
- ***SHA1Length*** specifies the length in characters of the SHA-1 digest value for a file entry.
- ***FileEntry*** specifies the filename of a file entry in the JAR Manifest file.
- ***Size*** specifies the size in bytes of a filename or digest value.
- ***Digest*** specifies the SHA-1 digest value of a file entry.

'[*JARFile*]', '[*ManifestFile*]', no 'Name: ' found

This condition indicates that a file entry was found but it did not include the file name. Each file entry must include the relative path of the file and a SHA-1 digest as shown in the example above.

'[*JARFile*]', '[*ManifestFile*]', no 'Name: ' found. Two consecutive new lines?

This condition indicates that the Manifest file is not formatted correctly. Each file entry must be separated by a blank line as shown in the example above. This condition indicates that more than one blank line exists between file entries.

'[*JARFile*]', '[*JARManifestFile*]', unexpected SHA1-Digest size of ([*SHA1Length*]) for entry '[*FileEntry*]'

This condition indicates that the SHA-1 Digest value for the entry specified is either too long or too short and likely incorrect.

'[*JARFile*]', '[*JARManifestFile*]': PGPND failed

Since the SHA-1 value is encoded, memory is allocated in order to decode the SHA-1 value. This condition indicates that a memory allocation error occurred.

'[*JARFile*]', '[*JARManifestFile*]', unexpected size ([*SHA1Length*]) for entry '[*FileEntry*]'

When the SHA-1 value is decoded, this condition indicates that the resulting SHA-1 value is either too long or too short and likely does not match the file entry.

'[*JARFile*]', '[*JARManifestFile*]', entry '[*FileEntry*]' not found

This condition indicates that a file entry was not found in the JAR Manifest file.

'[*JARFile*]', '[*JARManifestFile*]', entry '[*FileEntry*]' hash error

This condition indicates that an error occurred while validating the hash value for the file entry.

'[*JARFile*]', '[*JARManifestFile*]', '[*FileEntry*]', ([*Size*]) byte(s) digest '[*Digest*]'

This condition indicates that an unexpected error occurred in a file entry.

Severity

The file entries in the Manifest file include a SHA-1 Digest for the files inside the JAR file. If this file is not formatted correctly, then the files cannot be authenticated. Therefore, this condition is an ERROR.

Cause

This problem typically occurs in authoring of the image.

Solution

The image must be re-authored.

Type:	Blu-ray
Reference:	Blu-ray Specifications, Section 3-2: BD-Java Specifications
Default Program Action:	Error

Rule ID: 1635

JAR Signature Block File analysis error

This is a general error message that is triggered when analyzing the JAR Signature file. For the specific cause of this error, please check the message in the **Additional Info** column in the Analysis. The possible causes of this error are listed and described in the **Additional Info** section.

Background

A JAR File includes a single Manifest file which contains a list of all the files in the JAR File (excluding the Manifest file itself) and a message digest for each. The JAR Manifest File is stored in the directory META-INF inside the JAR File. The Manifest file includes a main section followed by a list of entries for each file inside the JAR file. Each file entry includes a filename and a SHA1-Digest for the file. An entry must exist for each signed file inside the JAR File.

Along with the Manifest file there is a Signature file (SIG-BD00.SF). The Signature file has a structure similar to the Manifest file in that it also includes entries for each file inside the JAR file. However, each complete file entry (Name & SHA1-Digest) in the Manifest file is hashed and the resulting digest is stored i the matching file entry in the Signature file.

The contents of the Signature file are 'signed' and the signature is stored in a certificate inside the Signature Block File (SIG-BD00.RSA). This rule is triggered when errors occur while analyzing the contents of the Signature Block File. The Signature Block File syntax is as follows:

Signature Block File Syntax	
Content Info	
Content Type	Identifies the content structure of the Signature Block File. In Blu-ray, this specifies "Signed Data".
Content	This field is a structure that describes the contents of the Signature Block File. The structure depends on the Content Type field. When the Content Type specifies "Signed Data", this field has the syntax as described in the following table.

Content Syntax		
Version	= "1"	
Digest Algorithm Identifier	= "SHA-1"	
Content Info	This field is a structure similar to the one above. However, when it is inside a Content structure, the Content Type must be set to "Data" and the Content is the Signature File contents.	
	Content Type	= "Data"
	Content	Signature File contents.
Certificates	One or more certificate chains.	
Signer Info	A structure that identifies the signer and an encrypted digest for the Signature File. This structur has the syntax as described in the following table:	

Signer Info Syntax	
Version	= "1"
Issuer and Serial Number	Identifies the signer's certificate via the Issuer Distinguished Name and Issuer-specific Serial Number, both of which are also found in a certificate in the Certificates field of the Content.
Digest Algorithm	= "SHA-1". The algorithm used to generate a digest for the Signature File.
Digest Encryption Algorithm	= "RSA", the algorithm used to encrypt the digest for the Signature File.
Encrypted Digest	The encrypted digest for the Signature File.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display more details with one o the following messages.

'[*JARFile*]', '[*SignatureBlockFile*]': PGPNKS failed

This condition indicates an internal error while allocating memory for internal structures.

[*JARFile*]', '[*SignatureBlockFile*]': **No signature block file data: ([*Size*])**

This error condition indicates that the Signature Block file has no data or the size is incorrect.

[*JARFile*]', '[*SignatureBlockFile*]': **DM failed**

This condition indicates that an error occurred while trying to decode the contents of the Signature Block File.

[*JARFile*]', '[*SignatureBlockFile*]': **MT failed**

This condition indicates that the ***Content*** *does not exist inside the* ***ContentInfo*** *structure.*

[*JARFile*]', '[*SignatureBlockFile*]': **DSD failed**

This condition indicates that an error occurred while trying to decode ***Content*** *inside the* ***ContentInfo*** *structure.*

[*JARFile*]', '[*SignatureBlockFile*]': **VSD failed**

This condition indicates that the function that verifies the certificates inside the Signature Block File has returned an error. The nalysis should display other instances of this rule with other messages in the Additional Info column related to this condition.

[*JARFile*]', '[*SignatureBlockFile*]': **Unknown PKCS-7 content**

This condition indicates that the data stored in the Content field of the ContentInfo structure is not recognized. The data should e structured in a format known as PKCS-7.

[*JARFile*]', '[*SignatureBlockFile*]': **PKINECACs failed, pCertSet**

This condition indicates that an internal error occurred while trying to allocate memory for the certificates inside the ***Content*** *tructure.*

[*JARFile*]', '[*SignatureBlockFile*]': **PKINCRLs failed, crlSet**

This condition indicates that an internal error occurred while trying to allocate memory for the certificate revocation list inside the ***Content*** *structure.*

[*JARFile*]', '[*SignatureBlockFile*]': **PKINSIs failed, signerInfos**

This condition indicates that an internal error occurred while trying to allocate memory for the SignerInfo structure.

[*JARFile*]', '[*SignatureBlockFile*]': **PGPND failed, pCertSetOut**

This condition indicates that an internal error occurred while trying to allocate memory need to encode the certificate data.

[*JARFile*]', '[*SignatureBlockFile*]': **PKIPECACs failed**

This condition indicates that an internal error occurred encoding the certificate data.

[*JARFile*]', '[*SignatureBlockFile*]': **PGPASNUCs failed**

This condition indicates that an internal error occurred when translating the raw encoded certificate data into PKCS-7 Certificate structures.

[*JARFile*]', '[*SignatureBlockFile*]': **PGPND failed, signerInfos**

This condition indicates that an internal error occurred while trying to allocate memory need to encode the ***SignerInfo*** *data.*

'[*JARFile*]', '[*SignatureBlockFile*]': PKIPSIs failed

This condition indicates that an internal error occurred encoding the SignerInfo data.

'[*JARFile*]', '[*SignatureBlockFile*]': PGPASNUSIs failed

This condition indicates that an internal error occurred when translating the raw encoded SignerInfo data into a SignerInfo structure.

'[*JARFile*]', '[*SignatureBlockFile*]': PKCS-7 has no signerInfos

This condition indicates that the SignerInfo structure does not exist in the ContentInfo structure.

'[*JARFile*]', '[*SignatureBlockFile*]': GIV failed, issuerAndSerialNumber, signerInfo([*SerialNo*] | [*SignerInfoIdx*])

This condition indicates that an error occurred when trying to read the ***Serial Number*** *from the SignerInfo structure.*

'[*JARFile*]', '[*SignatureBlockFile*]': DNL2 failed, issuerAndSerialNumber, signerInfo([*SerialNo*] | [*SignerInfoIdx*])

This condition indicates that an error occurred when trying to determine the length of the ***Issuer*** *in the SignerInfo structure.*

'[*JARFile*]', '[*SignatureBlockFile*]': PGPND failed, issuerAndSerialNumber, signerInfo([*SerialNo*] | [*SignerInfoIdx*])

This condition indicates that an error occurred when trying to allocate memory to read the ***Issuer*** *from the SignerInfo structure.*

'[*JARFile*]', '[*SignatureBlockFile*]': DNL2 failed, issuerAndSerialNumber, signerInfo([*SerialNo*] | [*SignerInfoIdx*])

This condition indicates that an error occurred when trying to read the ***Issuer*** *from the SignerInfo structure.*

'[*JARFile*]', '[*SignatureBlockFile*]': GIV failed, serialNumber, cert([*SerialNo*] | *CertIdx*)

This condition indicates that an error occurred when trying to read the Serial Number from a tbsCertificate.

'[*JARFile*]', '[*SignatureBlockFile*]': VX509C failed, cert([*SerialNo*] | [*CertIdx*])

This condition indicates that the function that analyzes a Certificate has returned an error. It is likely that there will be other analysis errors related to this condition.

'[*JARFile*]', '[*SignatureBlockFile*]': Can't determine TBSCertificate size, cert([*SerialNo*] | *CertIdx*)

This condition occurs when trying to determine the size of a tbsCertificate.

'[*JARFile*]', '[*SignatureBlockFile*]': PGPND failed, certOut, cert([*SerialNo*] | [*CertIdx*])

This condition occurs when trying to allocate memory to encode the binary tbsCertificate data.

'[*JARFile*]', '[*SignatureBlockFile*]': PKIPTBSC failed, cert([*SerialNo*] | [*CertIdx*])

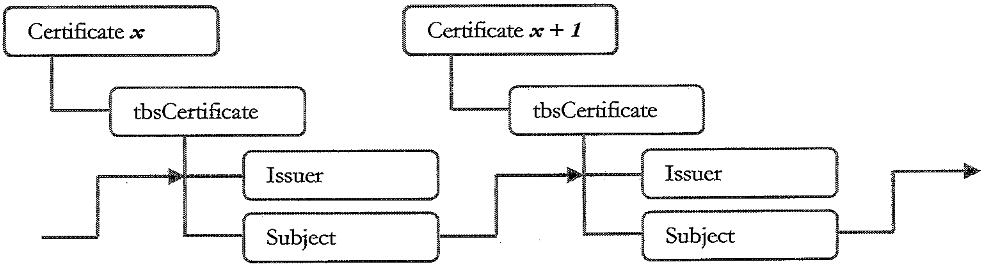
This condition occurs when trying to decode the binary tbsCertificate data info a tbsCertificate structure.

'[*JARFile*]', '[*SignatureBlockFile*]': URSAK failed, cert([*SerialNo*] | [*CertIdx*])

This condition occurs when trying to decode the Public Key from a tbsCertificate structure.

Issued by '[*Issuer*]' instead of '[*Subject*]'. '[*JARFile*]', '[*SignatureBlockFile*]': cert([*SerialNo*] | [*CertIdx*]), Issuer: '[*Issuer*]'

This condition occurs when the Issuer of a tbsCertificate is not equal to the Subject of the previous tbsCertificate. In a certificate chain, the Issuer of a certificate must be the Subject of its parent (previous) certificate.



Severity

The Signature Block File is used in the authentication of BD-Java applications and their related files. If the Signature Block File is nor formatted correctly, then BD-Java applications cannot be authenticated. Therefore, this condition is an ERROR.

Cause

This problem typically occurs in authoring of the image.

Solution

The image must be re-authored.

Type:	Blu-ray
Reference:	Blu-ray Specifications, Section 3-2: BD-Java Specifications
Default Program Action:	Error

Rule ID: 1637

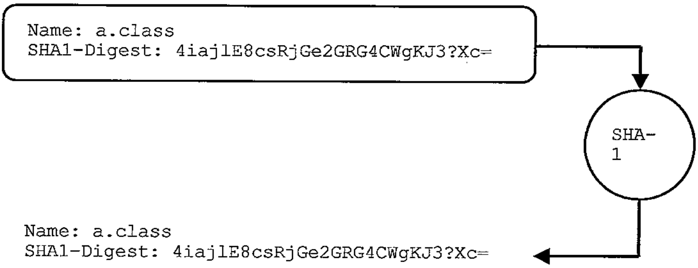
JAR Signature File analysis error

This is a general error message that is triggered when analyzing the JAR Signature file. For the specific cause of this error, please check the message in the **Additional Info** column in the Analysis. The possible causes of this error are listed and described in the **Additional Info** section.

Background

A JAR File includes a single Manifest file which contains a list of all the files in the JAR File (excluding the Manifest file itself) and a message digest for each. The JAR Manifest File is stored in the directory META-INF inside the JAR File. The Manifest file includes a main section followed by a list of entries for each file inside the JAR file. Each file entry includes a filename and a SHA1-Digest for the file. An entry must exist for each signed file inside the JAR File.

Along with the Manifest file there is a Signature file (SIG-BD00.SF). The Signature file has a structure similar to the Manifest file in that it also includes entries for each file inside the JAR file. However, each complete file entry (Name & SHA1-Digest) in the Manifest file is hashed and the resulting digest is stored in the matching file entry in the Signature file.



```
Name: a.class
SHA1-Digest: 4iajlE8csRjGe2GRG4CWgKJ3?Xc=
```

```
Name: a.class
SHA1-Digest: 4iajlE8csRjGe2GRG4CWgKJ3?Xc=
```

Additionally, the Signature file includes a digest for the Manifest file. The syntax of the Signature file is as follows:

Signature File Syntax	
Signature-Version:	These are the Main attributes in the Signature file required by BD-Java. The SHA1-Digest-Manifest attribute is the digest computed over the content of the JAR Manifest File.
BDJ-Signature-Version:	
Created-By:	Below the main section is a list of entries: one for each signed file inside the JAR File.
SHA1-Digest-Manifest:	
File Entries	The remaining sections are each an entry that identifies a file inside the JAR file. Each entry includes the following fields.
Name:	This is a relative path to a file inside the JAR file. This must match an entry with the same name in the Manifest File.
SHA1-Digest:	This is a SHA-1 digest value for the matching file entry in the Manifest file.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display more details with one of the following messages.

The following are error conditions that occur while checking main attributes:

'[*JARFile*]', '[*SignatureFile*]', 'Signature-Version' main attribute not specified

This condition indicates that the ***Signature-Version*** *was not specified. The JAR File Specifications require this attribute to be specified.*

'[*JARFile*]', '[*SignatureFile*]', 'BDJ-Signature-Version' main attribute not specified

This condition indicates that the ***BDJ-Signature-Version*** *was not specified. The BD-Java Specifications require this attribute to be specified.*

'[*JARFile*]', '[*SignatureFile*]', expecting '[*VersionAttribute*]' 1.0 instead of [*VersionAttriubte*] ([*ActualVersion*])

This condition indicates that the ***Signature-Version*** *is not version 1.0 as required by the JAR File Specifications.*

'[*JARFile*]', '[*SignatureFile*]', expecting '[*BDJVerAttribute*]' 1.0 instead of [*BDJVerAttribute*] ([*ActualVersion*])

This condition indicates that the ***BDJ-Signature-Version*** *is not version 1.0 as required by the BD-Java Specifications.*

'[*JARFile*]', '[*SignatureFile*]', expected SHA1-Digest-Manifest attribute found with no JAR Manifest file

This condition indicates that the ***SHA1-Digest-Manifest*** *attribute was specified and contains a valid value. However, the JAR Manifest file does not exist. The JAR Manifest file must be present in the META-INF directory of the JAR file. It is hashed and the resulting digest value is stored in the* ***SHA1-Digest-Manifest*** *attribute of the Signature file.*

'[*JARFile*]', '[*SignatureFile*]', unexpected SHA1-Digest size of ([*Size*]) for SHA1-Digest-Manifest

This condition indicates that the ***SHA1-Digest-Manifest*** *attribute contains a digest value with an invalid size and, therefore, it is likely that it is incorrect.*

'[*JARFile*]', '[*SignatureFile*]': PGPND failed for SHA1-Digest-Manifest

This condition indicates that an error occurred while trying to allocate memory to decode the SHA-1 Digest for the Manifest file.

'[*JARFile*]', '[*SignatureFile*]', unexpected size ([*Size*]) for SHA1-Digest-Manifest

This condition indicates that after decoding the SHA-1 Digest for the Manifest file, the length of the digest is incorrect.

'[*JARFile*]', '[*SignatureFile*]', '[*JARManifestFile*]' hash error

This condition indicates that an error occurred when trying to validate the SHA-1 digest for the JAR Manifest File.

'[*JARFile*]', '[*SignatureFile*]','[*JARManifestFile*]', ([*FileSize*]) byte(s), digest '[*DigestValue*]'

This condition indicates that an error occurred when trying to validate the SHA-1 digest for the JAR Manifest File.

The following are error conditions that occur while checking individual file entries:

'[*JARFile*]', '[*SignatureFile*]', unexpected SHA1-Digest size of ([*DigestLength*]) for entry '[*FileEntry*]'

This condition indicates that the SHA-1 Digest value for a file entry is the wrong length.

'[*JARFile*]', '[*SignatureFile*]': PGPND failed

This condition indicates an internal error when trying to allocate memory for decoding the SHA-1 Digest value for a file entry.

'[*JARFile*]', '[*SignatureFile*]', unexpected size ([*Size*]) for entry '[*FileEntry*]'

This condition indicates that the SHA-1 Digest value for the entry specified is either too long or too short and likely incorrect.

'[*JARFile*]', '[*SignatureFile*]', error while locating JAR Manifest file entry '[*FileEntry*]'

This condition indicates that an error occurred while searching for the file entry in the JAR Manifest file. Both JAR Manifest and Signature files must have matching file entries.

'[*JARFile*]', '[*SignatureFile*]', JAR Manifest file entry '[*FileEntry*]' not found

This condition indicates that the JAR Manifest file does not include a matching file entry. Both JAR Manifest and Signature files must have matching file entries.

'[*JARFile*]', '[*SignatureFile*]', entry '[*FileEntry*]' hash error

This condition indicates an error while trying to validate the hash for a file entry.

'[*JARFile*]', '[*SignatureFile*]', '[*FileEntry*]', ([*Size*]) byte(s), digest '[*Digest*]'

This condition indicates that an unexpected error occurred in a file entry.

Severity

The file entries in the Signature file include a SHA-1 Digest for the entries inside the JAR Manifest file. If this file is not formatted correctly, then the files cannot be authenticated. Therefore, this condition is an ERROR.

Cause

This problem typically occurs in authoring of the image.

Solution

The image must be re-authored.

Type:	Blu-ray
Reference:	Blu-ray Specifications, Section 3-2: BD-Java Specifications
Default Program Action:	Error

Rule ID: 1636

Key Conversion Data length is not 32 characters

The Key Conversion Data in the AACS1.DAT or BDCMF.CMF file is not the correct length.

Background

Key Conversion Data (KCD) is used as part of the protection of the contents of a Blu-ray image. The KCD is combined with a device key to obtain a Media Key. The Media Key can be used to un-encrypt the CPS Unit keys, which are then used to un-encrypt the Clip AV data files.

On a BDCMF image, the KCD is stored as a hexadecimal value:

```
<KCD>1234123412341234123412341234123412341234</KCD>
```

Depending on the BDCMF version, the KCD may be stored in the AACS1.DAT file (BDCMF 0.90) or in the BDCMF.CMF file (BDCMF 1.01). The KCD is mandatory for Type C and Type D images.

Once the KCD is used to obtain a Media Key, the Media Key is used together with the Volume ID (VID) and both are sent to the Rom-Mark Inserter (RMI). The RMI is the device that records the Rom-Mark onto the media.

When the KCD is not the proper length, it indicates a serious error as it cannot be used to obtain a Media Key, and therefore, the CPS Unit keys cannot be un-encrypted and the media will be unplayable.

Severity

This condition indicates a serious problem when the BD image is Type C or Type D. It is likely that an image with this error may abort during the mastering process.

Cause

This problem is typically introduced during the authoring process of the image. The authoring system is responsible for generating and recording the KCD in the BDCMF.CMC or AACS1.DAT files.

Solution

This problem cannot be corrected during pre-mastering or mastering process. The image must be re-authored.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

Rule ID: 1433

Key Conversion Data not verified

The AACS Type A key was not found. Therefore, the Key Conversion Data was not been verified.

Background

Key Conversion Data (KCD) is a key that is used on encrypted BD and HD images. This key is used to obtain other keys that are used to un-encrypt an image prior to playback. During analysis of an encrypted BD/HD image, the EclipseSuite tools will verify the KCD. However, to verify the KCD, the EclipseSuite tools require that the AACS Type A key be present in the same directory as the EclipseSuite tools. If the AACS Type A key is present and the KCD is verified, then the rule 'Key Conversion Data verified' is triggered. If the AACS Type A key is not present, then this rule is be triggered.

Severity

This is an informational message that notifies the user that the KCD has NOT been verified. There is the possibility that if the KCD is invalid, it may cause playability problems on a BD/HD disc.

Cause

The KCD is created/specified by the authoring system when the image is authored.

Solution

The image must be re-authored or the CDF/BDCMF files must be updated with the correct KCD.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Flag

Rule ID: 1511

Key Conversion Data verified

The Key Conversion Data has been verified to be correct.

Background

Key Conversion Data (KCD) is a key that is used on encrypted BD and HD images. This key is used to obtain other keys that are used to un-encrypt an image prior to playback. During analysis of an encrypted BD/HD image, the EclipseSuite tools will verify the KCD. However, to verify the KCD, the EclipseSuite tools require that the AACS Type A key be present in the same directory as the EclipseSuite tools. If the AACS Type A key is present and the KCD is verified, then this rule is triggered. If the AACS Type A key is not present, then the rule 'Key Conversion Data not verified' is triggered.

Severity

This is an informational message that notifies the user that the KCD has been verified. It does not indicate an error.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Info

Rule ID: 1510

Layer 1 PAC contains data

The PAC Specific Information field of the PACL1.DAT file contains non-zero data. It is a requirement that the PAC Specific Information fields of PAC Clusters in Layer 1 be set to 00h.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Flag

Rule ID: 1460

M2TS file overlaps with more than one SSIF file

An M2TS file cannot overlap with more than one SSIF file.

Background

In 3D, each SSIF file is associated with two M2TS files: one for the left eye and one for the right eye. The SSIF file consists (overlaps) of extents from each of the two M2TS files (SSIF = L + R). The SSIF file is created in such a way that it includes data from both left and right eye M2TS files. Therefore, the SSIF file must include extents from at two different M2TS files.

Severity

It is unknown how this condition might affect playability. Therefore, it is treated as an ERROR.

Cause

This condition is caused by the authoring system that created the image.

Solution

The image must be authored. However, as of this writing, the 3D specifications were not yet finalized. Check with the author of the image to verify the severity of this condition.

Type:	3D-BD
Reference:	3D Specifications
Default Program Action:	Error

Rule ID: 1734

M2TS Specific Area not aligned with AU

The start and end address of an M2TS Specific Area must be a multiple of an Aligned Unit.

Background

A 3D BD image may have both 2D and 3D files (*.M2TS and *.SSIF). These files overlap in some areas. The areas of an M2TS file that do not overlap with an SSIF file are called 'M2TS Specific Areas'. The specifications require that the start and end address of M2TS Specific Areas be a multiple of an Aligned Unit. This rule is triggered if they are not.

Severity

The default severity of this condition is an ERROR. However, it is unknown if this condition affects playability.

Cause

The cause of this condition is the authoring system that created the image.

Solution

It is unknown if this condition causes any problems.

> **NOTE!**
> *The 3D BD format is still under development and specifications are yet to be finalized. You should consult with the authors of the image or Eclipse Support for further assistance.*

Type:	3D-BD
Reference:	3D BD Specifications
Default Program Action:	Error

Rule ID: 1724

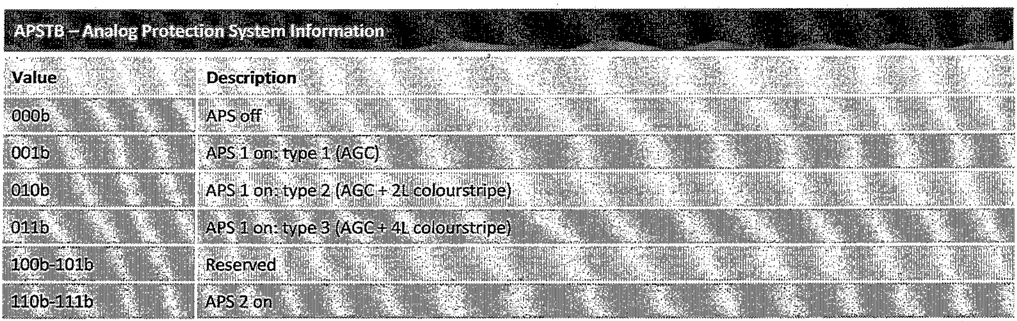
Macrovision Error

The bits that describe the Macrovision APS protection status have an invalid value.

Background

The Analog Protection System is specified in the **Basic CCI for AACS** structure of a CPS Unit Usage File.

This structure is used to specify the protection status of a CPS Unit. There are different protection systems that can be applied to a BD image including AACS and Macrovision APS. This error is triggered when the Macrovision APS bits are set to a reserved value (100b-101b).



APSTB – Analog Protection System Information

Value	Description
000b	APS off
001b	APS 1 on: type 1 (AGC)
010b	APS 1 on: type 2 (AGC + 2L colourstripe)
011b	APS 1 on: type 3 (AGC + 4L colourstripe)
100b-101b	Reserved
110b-111b	APS 2 on

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display the value that was found with the following message:

INVALID APS BITS ([value])

This message shows the value of the APS bits that was found.

Severity

This rule is considered an error since the APSTB bits are incorrect. It is unknown how this may affect playability.

Cause

This problem is typically caused by the authoring system that created the image.

Solution

The image must be re-authored.

Type:	Blu-ray
Reference:	AACS Blu-ray Pre-recorded Book Revision 0.92
Default Program Action:	Error

Rule ID: 1603

Managed Copy - Image not compliant

The Blu-ray image is not Managed Copy ready.

Background

Starting in the second quarter of 2010, all Blu-ray Video titles must support Managed Copy. This is a requirement of the AACS licensing agreement. Therefore, anyone producing Blu-ray Video titles (authoring, replicating, etc.) must ensure that they are Managed Copy ready.

> **NOTE!**
> *There are some exceptions which will allow images not to comply with this requirement. Please refer to your AACS Licensing agreement for more details.*

A Blu-ray Video that is Managed Copy ready must include a Managed Copy Manifest File (MCMF.XML). This file includes an ISAN number to perform the Managed Copy online transaction and a URI address for the Managed Copy server. If an URI is not specified, then the connection is to a default Managed Copy server.

The EclipseSuite tools include several rules that may be triggered when determining if a BD image is Managed Copy compliant. They are as follows:

Rule	Severity
Managed Copy Compliant (*None of the rules below will be triggered*)	Info
Managed Copy - Image not compliant (*Any of the below rules will trigger this rule*)	Error
No AACS Managed Copy Manifest File	Warning
AACS Managed Copy Manifest File error	Warning
ISAN error	Warning
BDCMF VISAN error	Warning

Severity

This condition is considered an ERROR since it is a requirement of the AACS Licensing agreement. However, this can be ignored on images that are exempt from this requirement.

Cause

This problem is typically caused by authoring.

Solution

If this image was intended to be Managed Copy compliant, then it must be re-authored. Contact the author to confirm or Eclipse Support for further assistance.

Type:	Blu-ray
Reference:	AACS Specifications
Default Program Action:	Error

Rule ID: 1752

Managed Copy compliant

This is an informational message that indicates that the Blu-ray image is Managed Copy ready.

Background

Starting in the second quarter of 2010, all Blu-ray Video titles must support Managed Copy. This is a requirement of the AACS licensing agreement. Therefore, anyone producing Blu-ray Video titles (authoring, replicating, etc.) must ensure that they are Managed Copy ready.

NOTE!
There are some exceptions which will allow images not to comply with this requirement. Please refer to your AACS Licensing agreement for more details.

A Blu-ray Video that is Managed Copy ready must include a Managed Copy Manifest File (MCMF.XML). This file includes an ISAN number to perform the Managed Copy online transaction and a URI address for the Managed Copy server. If an URI is not specified, then the connection is to a default Managed Copy server.

The EclipseSuite tools include several rules that may be triggered when determining if a BD image is Managed Copy compliant. They are as follows:

Rule	Severity
Managed Copy Compliant (*None of the rules below will be triggered*)	**Info**
Managed Copy - Image not compliant (*Any of the below rules will trigger this rule*)	**Error**
No AACS Managed Copy Manifest File	Warning
AACS Managed Copy Manifest File error	Warning
ISAN error	Warning
BDCMF VISAN error	Warning

Type:	Blu-ray
Reference:	AACS Specifications
Default Program Action:	Info

Rule ID: 1751

Managed Copy Manifest file - No URI found

This is an informational message that indicates that the Managed Copy Manifest File (MCMF.XML) does not include a URI to a Managed Copy server. If the image is Managed Copy compliant, then the 'default server' can be used for the Managed Copy operations, as defined by the AACS specifications.

Background

Starting in the second quarter of 2010, all Blu-ray Video titles must support Managed Copy. This is a requirement of the AACS licensing agreement. Therefore, anyone producing Blu-ray Video titles (authoring, replicating, etc.) must ensure that they are Managed Copy ready.

NOTE!
There are some exceptions which will allow images not to comply with this requirement. Please refer to your AACS Licensing agreement for more details.

A Blu-ray Video that is Managed Copy ready must include a Managed Copy Manifest File (MCMF.XML).

This file includes an ISAN number to perform the Managed Copy online transaction and a URI address for the Managed Copy server. If an URI is not specified, then the connection is to a default Managed Copy server.

The EclipseSuite tools include several rules that may be triggered when determining if a BD image is Managed Copy compliant. They are as follows:

Rule	Severity
Managed Copy Compliant (*None of the rules below will be triggered*)	Info
Managed Copy - Image not compliant (*Any of the below rules will trigger this rule*)	Error
No AACS Managed Copy Manifest File	Warning
AACS Managed Copy Manifest File error	Warning
ISAN error	Warning
BDCMF VISAN error	Warning

Type: Blu-ray
Reference: AACS
Default Program Action: Info

Rule ID: 1750

Managed Copy URI

This is an information rule that identifies the URI of the Managed Copy server.

Type: Blu-ray
Reference: AACS Blu-ray Disc Pre-recorded Book 0.951
Default Program Action: Info

Rule ID: 1793

Maximum inter-layer jump distance exceeded

The maximum jump distance between layers has been exceeded.

Background

In order to guarantee seamless playback of PlayItems, the Blu-ray specifications for 3D requires that the jump distance of a PlayItem between each extent of Stereoscopic Interleaved file between layers be less than 40000 logical sectors.

Severity

It is unknown how this may affect playability. Therefore, this condition is treated as an ERROR.

Cause

This condition is caused by the authoring system that created the image.

Solution

The image must be re-authored. Contact Eclipse Support for further assistance.

Type:	Blu-ray
Reference:	Blu-ray Specifications Annex 9: Main requirements for Stereoscopic 3D
Default Program Action:	Error

Rule ID: 1775

Maximum intra-layer jump distance exceeded

The maximum jump distance within a layer has been exceeded.

Background

In order to guarantee seamless playback of PlayItems, the Blu-ray specifications for 3D requires that the jump distance of a PlayItem between each extent of Stereoscopic Interleaved file within the same layer be less than 640000 logical sectors.

Severity

It is unknown how this may affect playability. Therefore, this condition is treated as an ERROR.

Cause

This condition is caused by the authoring system that created the image.

Solution

The image must be re-authored. Contact Eclipse Support for further assistance.

Type:	Blu-ray
Reference:	Blu-ray Specifications Annex P: Main requirements for Stereoscopic 3D
Default Program Action:	Error

Rule ID: 1774

Maximum Stereoscopic average bitrate exceeded

A left and right eye extent pair has exceeded the maximum bit rate allowed.

Background

A Stereoscopic Interleaved file (SSIF) consists of extents from the left and right eye Clip AV files. For each extent from the left eye file there is an extent from the right eye. The specifications require that the sum of the average bit rate of each extent be less than or equal to $64*10^6$ bits/second. The bit rate is calculated on every pair of extents (left & right eye).

Severity

It may be possible that if the bit rate is exceeded it may result in playability problems. Therefore, this rule is considered an ERROR.

Cause

This condition is caused by the authoring system that created the image.

Solution

The image must be re-authored. Contact Eclipse Support for further assistance.

Type:	3D
Reference:	Blu-ray Specifications Annex P: Main requirements for Stereoscopic 3D
Default Program Action:	Error

Rule ID: 1773

Missing Basic CCI for AACS

A CPS Unit Usage file is missing the Basic CCI for AACS.

Background

The Basic CCI is included as part of a CPS Unit Usage file (CPSUnitXXXXX.cci). It is a data structure that includes copy control information for a CPS Unit. It specifies items such as Copyright Control Information, Image Constraint Token, Digital Token Only and Analog Protection System. This rule indicates that the Basic CCI structure was not included as required by the AACS specifications.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will identify the CPS Unit that is missing this data.

Severity

This condition is considered an ERROR.

Cause

This condition is caused by the authoring application that created the image.

Solution

The image must be re-authored. Contact Eclipse Support for further assistance.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Info

Rule ID: 1868

Missing BDCMF LayerInfo L0SectorSize attribute

The L0SectorSize attribute of the LayerInfo element is missing.

Background

The mandatory BDCMF LayerInfo L0SectorSize attribute describes the total number of sectors of the data zone of layer 0. See the BDCMF.CMF example below.

```
<DiscInfo>
    <DiscType GeneralType="BD-ROM" BDType="BD" HybridType="NOHYBRID" DiscSize="12cm" />
    <LayerInfo Total="2" BD="2" L0SectorSize="4148224" />
    <BDInfo Density="25G" />
    <Note>This is a regular dual layer disc</Note>
</DiscInfo>
```

Possible Cause

This condition typically occurs when the image is created.

Severity

This rule is considered an error since it is not possible to process the image with this missing attribute.

Possible Solution

The image must be re-created.

Type:	Blu-ray
Reference:	BDCMF Specs 3.1.2.2
Default Program Action:	Error

Rule ID: 1403

Missing BDCMF LayerInfo L1SectorSize attribute

The L1SectorSize attribute of the LayerInfo element is missing.

Background

The mandatory BDCMF LayerInfo L1SectorSize attribute describes the total number of sectors of the data zone of layer 1. This information is required only on a Triple Layer BD image.

Severity

This rule is considered an error since it is not possible to process the image with this missing attribute.

Possible Solution

The image must be re-created.

Type:	Blu-ray
Reference:	None
Default Program Action:	Error

Rule ID: 1901

Missing BD-J application root certificate

The EclipseSuite tools were not able to find the application root certificate file.

Background

The Application root certificate is normally at the top level of the certificate chain. It is used to validate other certificates and it is assumed to be a 'trusted' certificate. This means that it does not have to be validated. The application root certificate file is stored in a file of its own (app_discroot.crt), whereas the rest of the certificates are stored in the Root Certificate File. However, a copy of the root certificate is also included in the root certificate file. When analyzing the certificate chain, the EclipseSuite tools analyze each certificate starting with the last certificate (leaf) and ending with the root certificate. The EclipseSuite certificate analysis checks all certificates including the root certificate. This error indicates that all certificates were analyzed and when attempting to analyze the application root certificate, it was detected that the root certificate file (\CERTIFICATE\app_discroot.crt) is missing.

Additional Info

When this error occurs, the **Additional Info** column in the analysis will display the following message.

'[*JARFile*]', '[*SignatureBlockFile*]': cert([*SerialNo*])

This message shows the JAR file, Signature Block filename and serial number of the certificate that was being analyzed when the error occurred.

Severity

The application root certificate is required for authentication of the BD-Java content. Therefore, this is considered an ERROR.

Cause

This problem typically occurs in authoring of the image.

Solution

The image must be re-authored.

Type:	Blu-ray
Reference:	Blu-ray Specifications, Section 3-2: BD-Java Specifications
Default Program Action:	Error

Rule ID: 1629

Missing Clip AV Stream file

A Clip AV file (#####.m2ts) is missing.

Background

During analysis of a Blu-ray video, the EclipseSuite tools validate that navigational structure of the video. The EclipseSuite tools build a list of all Clip files that are referenced in the navigational structure. This rule is triggered when the EclipseSuite tools find a reference to a Clip file but are unable to locate it in the UDF file structure of the image. It is possible that the reference is for a Clip file that can be downloaded from an online server.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will identify the Clip file.

Blu-ray Video: '[*Filename*]'

This message identifies the Clip AV Stream file that the EclipseSuite tools were unable to find. Contact the author of the image to confirm whether the file is intended to be downloaded from an online server. If so, then this warning can be ignored. Otherwise, it indicates a serious problem and the image must be re-authored.

Severity

Currently the EclipseSuite tools are not able to determine if the Clip file is supposed to be present on the image or if it is a file that will be downloaded from an online server. For this reason, it is considered only a WARNING. You should contact the author and find out whether the file was intended to be downloaded or if it supposed to be present on the image.

Cause

This is caused by the authoring application that created the image.

Solution

This may be a condition that is ok as long as the Clip file was intended to be downloaded from an online server. However, you should contact the author to confirm. If the file should is supposed to be recorded on the image, then the image must be re-authored.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Warning

Rule ID: 1592

Missing link in TBS certificate chain

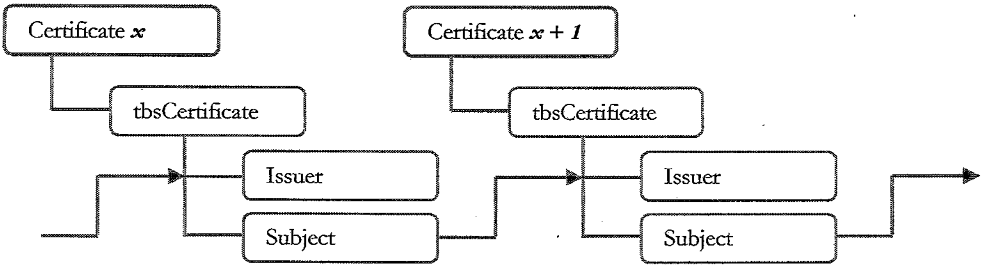
There is a missing certificate in the certificate chain.

Background

To validate that BD-Java applications and related files have not been compromised, authors provide a digital signature in certificates inside the Signature Block File. The EclipseSuite tools analyze all certificates and their digital signatures to make sure they match the BD-Java content on the image.

The Signature Block File includes a certificate chain starting with the application root certificate and ending with the leaf certificate that contains the digital signature that is used to authenticate the BD-Java content. As part of the BD-Java Security Analysis, the EclipseSuite validate the certificate chain.

In a tbsCertificate, it is the Issuer and Subject fields that link one certificate to another. For example, the Issuer field is the same as the Subject field of the previous certificate. Since the root certificate is at the top level of the certificate chain, both Issuer and Subject fields are the same.



Additional Info

When this error occurs, the **Additional Info** column in the Analysis will display more details with one of the following messages.

Issued by '[*Issuer*]' instead of '[*Subject*]'. '[*JARFile*]', '[*SignatureBlockFile*]': cert([*SerialNo*] | [*CertIdx*]), Issuer: '[*Issuer*]'

*This message identifies the **Issuer** of a certificate. The **Issuer** field must be the same as the **Subject** field in the previous certificate in the chain. When the Issuer is not equal to the Subject of the previous certificate, then it is assumed that there is a missing link (certificate).*

This message also identifies the JAR file and Signature Block file that contain the certificates that are being analyzed. The Serial Number, Certificate Index and Issuer fields identify the certificate that was being analyzed when this error condition occurred.

Issued by '[*Subject*]'. '[*JARFile*]', '[*SignatureBlockFile*]': cert([*SerialNo*] | [*CertIdx*]), Issuer: '[*Issuer*]'

*The current certificate identifies **Subject** as the entity that issued the certificate. Therefore, there must be a certificate whose **Issuer** field equals the **Subject** field of the current certificate. However, there is no 'parent' certificate above the current certificate. This also implies that there is no root certificate since it is expected that the root certificate is at the top of the certificate chain. In the case of the root certificate, both **Issuer** and **Subject** fields should be the same.*

Severity

If the certificate chain is not complete, then authentication cannot be completed and will be considered failed. Therefore, this is considered an ERROR.

Cause

This problem typically occurs in authoring of the image.

Solution

The image must be re-authored.

Type:	Blu-ray
Reference:	Blu-ray Specifications, Section 3-2: BD-Java Specifications
Default Program Action:	Error

Rule ID: 1631

Missing Movie Object

The explanation for this title check rule contains confidential information. Please refer to the studio-specific supplemental rules help PDF document. The document is available from Eclipse Support.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

Rule ID: 1748

Missing required AACS file

One of the required AACS files was not found.

Background

When a Blu-ray image is protected with AACS, there are several files that must be present in the image. This rule is triggered if any of them are missing.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display more details.

[Filename]

This message identifies the filename that was not found.

'*[OriginalFilename]*' and '*[ExpectedFilename]*' differ in letter case

This message indicates that the file was found but unfortunately the filename character casing does not comply with the specifications.

Severity

The required AACS files are critical in the processing of an AACS-protected image. If one of them is missing, it may not be possible to process the image. Therefore, this condition is considered an ERROR.

Cause

This condition is normally caused by the authoring system that created the image.

Solution

The image needs to be re-authored. Contact Eclipse Support for further assistance.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

Rule ID: 1662

Missing Top Menu

The Blu-ray disc or image is missing a Top Menu.

Early BD-ray players may experience playability problems if a disc does not include a Top Menu. Although this may not be a problem with current players or current versions of the player firmware, this rule still exists in case an old player with old firmware is used to play a disc without a Top Menu.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Warning

Rule ID: 875

MKB and BDCMF Media Key (Km) mismatch

The Media Key (Km) that is stored in the BDCMF file-set is different from the one stored in the MKB_RO.inf in the image.

Background

Blu-ray Video images include this file in the \AACS folder. However, when the image is Type A or B, file is just a placeholder for the real file that is sent from AACS LA. When the image is signed (i.e. conversion from Type B to Type C), the file in the image is replaced with the file from AACS LA. Inside this file is the Media Key, which is also written to one of the BDCMF files (AACS1.DAT when using BDCMF version 0.90 and BDCMF.CMF when using version 1.0x). During the analysis of a Type C or Type D image, the EclipseSuite tools compare the Media Key from the BDCMF and the MKB_RO.inf file. When they do not match this rule is triggered.

Severity

This rule is considered an ERROR since it is possible that it may lead to playability problems.

Cause

It is unknown as to the cause of this error.

Solution

Contact Eclipse Customer Support for further assistance.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

Rule ID: 1594

MKB Process Error

An error occurred while trying to process the Media Key Block file.

Background

The Media Key Block file is essential for the playability of Blu-ray images.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display details about the condition that triggered this rule.

File not found '[*filename*]'

This condition indicates that the EclipseSuite tools were unable to locate the Media Key Block file(s).

There are two MKB files in the Blu-ray format: the Read-Only Media Key Block filename is MKB_RO.inf, and the Read/Write Media Key Block filename is MKB_RW.inf.

Failed to read '[*filename*]'

This condition indicates that the EclipseSuite tools found the Media Key Block file(s) but was unable to load the file(s) into memory.

There are two MKB files in the Blu-ray format: the Read-Only Media Key Block filename is MKB_RO.inf, and the Read/Write Media Key Block filename is MKB_RW.inf.

Bad Pre-recorded records

The Media Key Block file contains records with different types of information. This message indicates that one or more records:

- *are missing*
- *have the wrong length*
- *have the wrong content*

On a Blu-ray image, the file this condition refers to is MKB_RO.inf.

Bad Recorder records

The Media Key Block file contains records with different types of information. This message indicates that one or more records:

- *are missing*
- *have the wrong length*
- *have the wrong content*

On a Blu-ray image, the file this condition refers to is MKB_RW.inf.

Record (*0xN*) not found

This condition indicates that the Media Key Block file is missing a record.

Record (*0xN*) overflow

This message indicates that a record length is invalid. A record's length must be within the Media Key Block file.

Device Key file not available. Contact Support

This is an unexpected error. Please save the log file and email it to support@eclipsedata.com.

Device keys have been revoked

The EclipseSuite programs require a device key when analyzing an encrypted Blu-ray disc or image. The device keys have an expiration period. If this condition occurs, it is likely that the key being used has expired. Contact Eclipse Customer Support for further assistance.

Device Keys don't apply

This condition typically occurs when the device keys in use have expired. Contact Eclipse Customer Support for further assistance.

Contact Support. Error is (*0xN*)

This is an unexpected error. Please save the log file and email it to support@eclipsedata.com.

This message will display an error number which will help in finding the cause of the error.

Type: HD DVD
Reference: AACS Blu-ray Disc Prerecorded Book
Default Program Action: Error

Rule ID: 847

Movie Studio

This is an informational message that identifies the movie studio that owns the Blu-ray Video image.

Background

This rule is part of the Title Structure analysis of EclipseSuite. The Title Structure analysis includes a list of movie studios that are supported. When the Title Structure analysis is being performed on an image, the movie studio is identified in the image and this rule is triggered to identify it in the EclipseSuite analysis.

Type: Blu-ray
Reference: N/A
Default Program Action: Info

Rule ID: 1621

Movie Studio required file missing

The explanation for this title check rule contains confidential information. Please refer to the studio-specific supplemental rules help PDF document. The document is available from Eclipse Support.

Type: Blu-ray
Reference: N/A
Default Program Action: Error

Rule ID: 1671

Multi-angle PlayItem requires at least two angles

A PlayItem was identified as multi-angle but it references less than 2 angles.

Background

A PlayItem structure includes a flag that specifies whether the PlayItem is 'multi-angle' (i.e. two or more angles). When a PlayItem is identified as 'multi-angle', the PlayItem structure includes additional data for each angle. This message indicates that a PlayItem was identified as 'multi-angle' but contains data for one or less angles.

Severity

It is unknown how this condition will affect playability. Therefore, it is treated as an ERROR.

Cause

This condition is caused by the authoring system that created the image.

Solution

The image must be re-authored. However, since the writing of this topic, the 3D Specifications were not finalized. Check with the author of the image to confirm the severity of this condition.

Type:	Blu-ray
Reference:	Blu-ray Specifications
Default Program Action:	Error

Rule ID: 1761

Multiple UTC-8 octet sequence

One of the XML image files contains an illegal character.

Background

XML documents include a field that specifies the encoding used by the document (i.e. file). Different encodings are used to specify different character sets required by different languages. The most common (and default for all XML image files) is UTF8. If an authoring application inserts a character that is not covered by UTF8, then this rule is triggered. This condition typically occurs when characters from other encodings (character sets) are used in a document formatted with UTF8. This will occur mostly in informational user-defined fields such as `<TitleInfo>` element of the BDCMF.CMF file. This element contains Title and Copyright information of the Blu-ray Video and it is these type of user-defined fields where this error would be expected.

Severity

This condition is considered INFO severity since it may not affect processing of the image.

Cause

This condition is typically caused by the authoring application that created the image. However, it is also possible that any other utility that edits the file may introduce characters that are not supported by the current encoding of the file.

Solution

Since this condition may not affect processing of the image it may be ignored. However, it still indicates the presence of a character not supported by the current encoding of the file.

Type:	Other
Reference:	XML Specifications
Default Program Action:	Info

Rule ID: 1777

Network connection not found

The explanation for this title check rule contains confidential information. Please refer to the studio-specific supplemental rules help PDF document. The document is available from Eclipse Support.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

Rule ID: 1651

No AACS Managed Copy Manifest File

The EclipseSuite programs were unable to find the Managed Copy Manifest File or the file is empty.

Background

The AACS specifications require that images that are Managed Copy ready include the Managed Copy Manifest File (mcmf.xml). During the analysis, the EclipseSuite programs check to make sure the file is present. If the file is not found or if the file is empty then this rule is triggered.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display more details with one of the following messages.

Can't find '[*Filename*]'

This condition indicates that the Managed Copy Manifest file is not included in the image. This file should be recorded in the \AACS and \AACS\DUPLICATE folders.

'[*Filename*]' is empty

This condition indicates that the Managed Copy Manifest file is present but it is empty.

Severity

The Managed Copy Manifest file is required for images that are Managed Copy ready. Therefore, it is possible that some images may not include it if they are not Managed Copy ready. This is considered a warning.

Cause

This condition is normally caused during authoring of the image.

Solution

Check with the author to see if the image is supposed to be Managed Copy ready. If so, then this image should be re-authored. If it is not Managed Copy ready, then the Managed Copy Manifest file should not have been included; in which case the image is ok to be processed.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Warning

Rule ID: 1719

No Clip AV Stream files

The EclipseSuite tools did not find any Clip AV Stream files for a CPS Unit.

Background

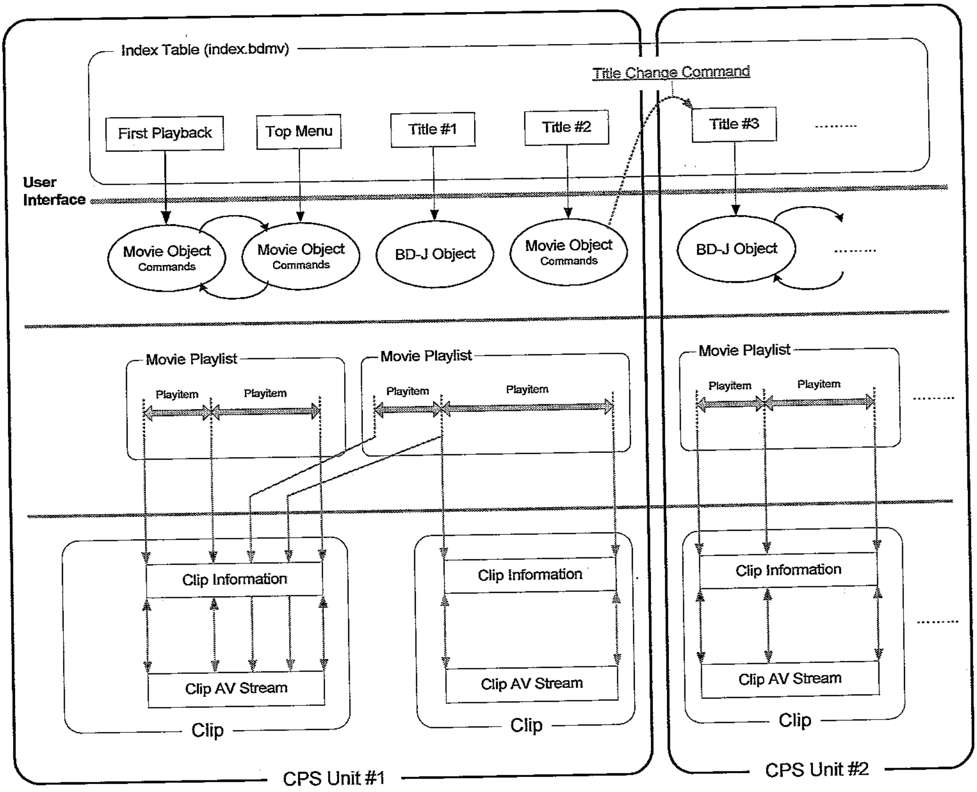
In the BD-ROM Video structure, the Index Table (index.bdmv) contains references to Titles. Titles contain Movie Objects or BD-J Objects. Movie Objects contain Commands which reference Playlists (*.mpls). Playlists include Playitems which reference Clips. A Clip references a Clip AV Stream file (*.m2ts).

The CPS Unit Key File (Unit_Key_RO.inf) also contains references to Titles in a BD-ROM Video as well as the Title Key assigned to each Title.

A CPS Unit identifies a group of Titles that are encrypted with the same Title Key (CPS Unit Key). This means that all Clips referenced Titles in the same CPS Unit are encrypted with the same Title Key.

On a Blu-ray disc, the EclipseSuite tools parse through the BD-ROM Video structure, as described above, in order to determine the number of Titles and the Clips referenced by each. On a BDCMF image, the BDCMF.CMF file includes CPS Unit elements and the Clips referenced by each.

This error indicates that a CPS Unit was found but did not include any references to Clip AV Stream files.


Index Table (index.bdmv)
Title Change Command
First Playback
Top Menu
Title #1
Title #2
Title #3
User Interface
Movie Object
Commands
Movie Object
Commands
BD-J Object
Movie Object
Commands
BD-J Object
Movie Playlist
PlayItem
PlayItem
Movie Playlist
PlayItem
PlayItem
Movie Playlist
PlayItem
PlayItem
Clip Information
Clip AV Stream
Clip
Clip Information
Clip AV Stream
Clip
Clip Information
Clip AV Stream
Clip
CPS Unit #1
CPS Unit #2

Severity

This rule is considered an ERROR since it indicates that the BD-ROM Video may not play at all.

Cause

This problem occurs in authoring since it is where the playback navigation structure is created.

Solution

This problem cannot be corrected in pre-mastering or mastering. The image must be re-authored.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

Rule ID: 1488

No Content ID in Managed Copy Manifest file

This is an informational message that indicates whether the 'Content ID' has been specified in the Managed

Copy Manifest File.

Background

The Content ID in the Managed Copy Manifest File is part of the ISAN number that is used for online transactions. In the current specifications, this field is optional. When the Content ID is not specified, then the Content Certificate ID is used instead.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Info

Rule ID: 1828

No corresponding EXT1 allocation for Base file

The Stereoscopic Interleaved file (SSIF) is missing an extent from the left view (2D) file.

Background

The Stereoscopic Interleaved file (SSIF) consists of extents from the left eye file (2D) and extents from the right eye file. The extents are paired so that for every extent from the left eye (EXT1) there is always an extent from the right eye (EXT2) and vice versa. This condition indicates that the SSIF file includes an extent from the right eye file without a matching extent from the left eye file.

Severity

It is possible that this condition may affect playability. Therefore, it is considered an ERROR.

Cause

This condition is caused by the authoring system that created the image.

Solution

The image must be re-authored. Contact Eclipse Support for further assistance.

Type:	3D
Reference:	Blu-ray Specifications Annex P: Main requirements for Stereoscopic 3D
Default Program Action:	Error

Rule ID: 1763

No corresponding EXT2 allocation for Dependent file

The Stereoscopic Interleaved file (SSIF) is missing an extent for the right eye file.

Background

The Stereoscopic Interleaved file (SSIF) consists of extents from the left eye file (2D) and extents from the right eye file. The extents are paired so that for every extent from the left eye (EXT1) there is always an extent from the right eye (EXT2) and vice versa. This condition indicates that the SSIF file includes an extent from the left eye file (2D) without a matching extent from the right eye.

Severity

It is possible that this condition may affect playability. Therefore, it is considered an ERROR.

Cause

This condition is caused by the authoring system that created the image.

Solution

The image must be re-authored. Contact Eclipse Support for further assistance.

Type:	3D
Reference:	Blu-ray Specifications Annex P: Main requirements for Stereoscopic 3D
Default Program Action:	Error

Rule ID: 1764

No history of ImageArchive BD record found in BDCMF

This is an informational message that indicated that a BDCMF image has not been previously archived to a database.

Background

When the BD Archive option is used, the Content Certificate Management Utility (CMU) automatically archives Type C images to a database. During this process, the CMU will add an entry into the process history of the BDCMF.CMF file, indicating that the image has been archived. This message indicates that the process history of an image does not include any history of being archived.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Flag

Rule ID: 1881

No Playing Time specified

The BDCMF image does not include the PLAYINGTIMEINFO attribute, which specifies the duration of each codec.

Background

This message is provided for informational purposes only and has no effect on the final disc. Nevertheless, it is a requirement by the BDCMF specifications and this rule is triggered when not included.

Severity

This attribute is required by the BDCMF specifications and there may be systems that expect it. The EclipseSuite tools report when it is missing with this rule but are not affected by it. Therefore, this is considered only a warning.

Cause

This problem is caused by the authoring application that created the image.

Solution

Since this problem does not have any effect in the processing of the image nor does it affect playability of the final disc, this rule can be ignored. However, if there are other external applications that rely on this information, then the author should consult with the makers of the authoring application to configure it so that it always generates this information.

Type:	Blu-ray
Reference:	BDCMF Specifications
Default Program Action:	Warning

Rule ID: 1903

No SSIF file detected

The image was detected to be a 3D BD but does not include a 3D-ready PlayList.

Background

A 3D BD image must include at least one 3D-ready PlayList. The PlayList includes PlayItems which reference the clip stream files that contain the actual audio/video presentation data. In the case of a 3D image, the audio/video information is stored in Stereoscopic Interleaved files (\STREAM\SSIF\*.SSIF). This rule indicates that the image was detected as a 3D BD but no SSIF files exist in the \STREAM\SSIF folder.

Additional Info

When this rule is triggered, the **Additional Info** column in the analysis will provide more details with one of the following messages.

But 3D ready PlayList(s) detected

The image includes a 3D-ready PlayList but no SSIF file exist. The PlayList file includes PlayItems, which contain references to the SSIF files.

*If the image is 3D BD, then it must be identified as such by the SS_content_exist_flag in the Index Table file (index.bdmv). The image must also include at least one 3D-ready PlayList. The stereoscopic interleaved files (*SSIF) that include the audio/video information must be recorded in the \STREAM\SSIF folder.*

Note: the presence of a 3D-ready PlayList alone does not identify the image as being 3D. The SS_content_exist_flag in the Index Table File (index.bdmv) must also be set. And, of course, the image must include SSIF files in the \STREAM\SSIF folder.

This condition is specific when a 3D-ready PlayList is detected but no SSIF files are found in the image.

But Index Table file 3D content flag set

The Index Table file (index.bdmv) identified the image as 3D BD but no SSIF files exist.

*The SS_content_exist_flag identifies an image as 3D Blu-ray Video image or a (2D) Blu-ray Video image. A 3D BD image must include at least one 3D-ready PlayList and one or more stereoscopic interleaved files (*SSIF).*

Severity

This condition is considered an ERROR since it is not clear if the image was intended to be a 3D BD.

Cause

This problem is typically caused by the authoring system that created the image.

Solution

The image must be re-authored to correct this problem.

NOTE!
The 3D BD format is still under development and specifications are yet to be finalized. You should consult with the authors of the image or Eclipse Support for further assistance.

Type:	3D-BD
Reference:	3D BD
Default Program Action:	Error

Rule ID: 1726

No XML Schema document in use

The EclipseSuite tools were not able to locate the XML Schema file to use when validating an XML file.

Background

When analyzing a BD image, the EclipseSuite tools will attempt to validate all XML files that are part of the image. In order to perform this validation, the XML Schema files must be present in the same directory from which the EclipseSuite programs are being executed.

On a Blu-ray image, the files BDCMF.CMF and AACS1.DAT files will be validated.

Blu-ray Schema Files

File Name	Schema File
BDCMF.CMF	CMF_[VER*]_[Type*].xsd
AACS1.DAT	AACS1_[VER*]_[Type*].xsd

[VER] represents the version of the BDCMF specifications. Every version is released with a new set of schema files.
[Type] represents each of the different BDCMF Types defined by the version of the BDCMF specifications.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will identify the XML file that is missing the schema.

XML file '[*filename*]'

This message identifies the Blu-ray XML file that the EclipseSuite tools were trying to validate.

Severity

This rule does not identify an error. It is simply an informational message that indicates that the EclipseSuite tools were unable to validate an XML file to make sure it conformed to a specific schema.

Cause

This problem occurs because the EclipseSuite tools were unable to locate the appropriate schema file(s). Either they don't exist or they are located in the wrong directory. The EclipseSuite tools require that the schema files be located in the same directory as the tools themselves.

Solution

Verify that the schema files are copied to the same directory as the EclipseSuite tools (example: C:\Eclipse\ImageTools50BD).

Type:	Other
Reference:	N/A
Default Program Action:	Info

Rule ID: 1517

Number of BD Titles

This is an informational rule, which displays the number of Blu-ray Titles in the Additional Info column of the analysis.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Info

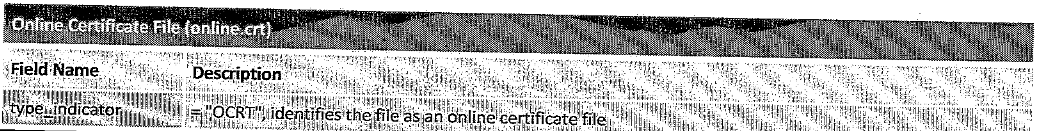
Rule ID: 864

Online certificate

This is an informational message that indicates that the online certificate is present.

Background

The Online certificate file (online.crt) is one of the components used for certification of network connections by BD-J applications when making network connections. This file is present only when a BD image includes and BD-J applications and it is stored in the \CERTIFICATE folder. During analysis of an image, the online certificate file is analyzed and its signature is validated.



Online Certificate File (online.crt)	
Field Name	**Description**
type_indicator	= "OCRT", identifies the file as an online certificate file

version_number	="0200", identifies the online certificate file version.	
reserved	= 00h	
Online Certificate	Certificate_version	="0", identifies the certificate version
	Content_owner_ID	Unique identifier of the online certificate issued by BDA-CA.
	Reserved	-00h
	Content_owner_name	Identifies the content owner as registered in BDA-CA.
	Content_owner_public_key	Identifies the content owner's public key issued by BDA-CA
	Certificate_signature	Digital signature of the fields from the start of the online certificate through Content_owner_public_key, signed by BDA-CA.

Type: Blu-ray

Reference: Blu-ray Disc Read-Only Format
Part 3: Audio Visual Basic Specifications Version 2.1
Amendments, 12 December 2007

Default Program Action: Info

Rule ID: 1588

Online certificate file error

The online certificate file contains an invalid value in one of its fields.

Background

The Online certificate file (online.crt) is one of the components used for certification of network connections by BD-J applications when making network connections. This file is present only when a BD image includes and BD-J applications and it is stored in the \CERTIFICATE folder. During analysis of an image, the online certificate file is analyzed and its signature is validated.

Online Certificate File (online.crt)

Field Name	Description	
type_indicator	= "OCRT", identifies the file as an online certificate file	
version_number	="0200", identifies the online certificate file version.	
reserved	= 00h	
Online Certificate	Certificate_version	="0", identifies the certificate version
	Content_owner_ID	Unique identifier of the online certificate issued by BDA-CA.
	Reserved	-00h
	Content_owner_name	Identifies the content owner as registered in BDA-CA.
	Content_owner_public_key	Identifies the content owner's public key issued by BDA-CA
	Certificate_signature	Digital signature of the fields from the start of the online certificate through Content_owner_public_key, signed by BDA-CA.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will identify the cause of this error with one of the following messages.

Type_indicator field is not 'OCRT'

The type_indicator field at the beginning of the file must have a value of 'OCRT' identifying the file as an online certificate file.

Version_number field is not '0200'

The version_number field must be set to '0200' identifying the version of the online certificate file.

Reserved field is not all zeros

The reserved field should be filled with zeros (00h). This condition is not critical since BD players should ignore all reserved fields.

Online_Certificate, Certificate_Version field is ([*Version*]) instead of zero

The Certificate Version field for the online certificate must be set to '0'.

Severity

This rule is considered an ERROR since most of the conditions listed above indicate incorrect file format. Without a correct online certificate file the user may not be able to run certain BD-J applications.

Cause

This problem is caused by the authoring system that created the image.

Solution

Contact Eclipse Customer Support for further assistance. It is likely that the image may need to be re-authored.

Type:	Blu-ray
Reference:	Blu-ray Disc Read-Only Format Part 3: Audio Visual Basic Specifications Version 2.1 Amendments, 12 December 2007
Default Program Action:	Error

Rule ID: 1590

Online certificate revocation list

This is an informational message that indicates that the online certificate revocation list file is present and its digital signature is valid.

Background

The Online certificate revocation list file (online.crl) is one of the components used for certification of network connections by BD-J applications. This file is present only when a BD image includes BD-J applications and it is stored in the \CERTIFICATE folder. During analysis of an image, the online certificate revocation list file is analyzed and its signature is validated.

Online Certificate Revocation List File (online.crl)

Field Name	Description	
type_indicator	= "OCRL", identifies the file as an online certificate revocation list file.	
version_number	="0200", identifies the online certificate revocation list file version.	
reserved	= 00h	
Online_CRL	Online_CRL_Version	= '0', identifies the certificate version.
	Number_of_Revocation	Number of revoked content owner's ID records. Each record includes the following fields.
	Revoked_contnet_ownder_ID	The content owner ID value in the revoked online certificate.
	Revocation_type	= 00 00h, indicating 'online certificate revocation'.
	Revocation_date	The revocation data as the elapsed date since January 01, 2008. The value 0x0001 = January 01, 2008, 0x0002 = January 02, 2008, etc.
	Online_CRL_Signature	Digital signature of the fields from the start of the online certificate revocation list file to the byte just before the Online_CRL_Signature field, signed by BDA-CA.
	Padding	= 00h

Type:	Blu-ray
Reference:	Blu-ray Disc Read-Only Format Part 3: Audio Visual Basic Specifications Version 2.1 Amendments, 12 December 2007
Default Program Action:	Info

Rule ID: 1598

Online certificate revocation list file error

The online certificate revocation list file contains invalid data.

Background

The Online certificate revocation list file (online.crl) is one of the components used for certification of network connections by BD-J applications. This file is present only when a BD image includes BD-J applications and it is stored in the \CERTIFICATE folder. During analysis of an image, the online certificate revocation list file is analyzed and its signature is validated.

Online Certificate Revocation List File (online.crl)

Field Name	Description	
type_indicator	= "OCRL", identifies the file as an online certificate revocation list file.	
version_number	="0200", identifies the online certificate revocation list file version.	
reserved	= 00h	
Online_CRL	Online_CRL_Version	= '0', identifies the certificate version.
	Number_of_Revocation	Number of revoked content owner's ID records. Each record includes the following fields.

	Revoked_contnet_ownder_ID	The content owner ID value in the revoked online certificate.
	Revocation_type	= 00 00h, indicating 'online certificate revocation'.
	Revocation_date	The revocation data as the elapsed date since January 01, 2008. The value 0x0001 = January 01, 2008, 0x0002 = January 02, 2008, etc.
	Online_CRL_Signature	Digital signature of the fields from the start of the online certificate revocatio list file to the byte just before the Online_CRL_Signature field, signed by BDA-CA.
	Padding	= 00h

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display the invalid data that triggered this rule with one of the following messages.

Type_indicator field is not 'OCRL'

The file 'online.crl' must start with the value 'OCRL' identifying it as an online certificate revocation list file.

Version_number field is not '0200'

The version of the online certificate revocation list file must be set to '0200'.

Reserved field is not all zeros

All reserved fields must be filled with zeros. However, this is not critical since BD players should ignore reserved fields.

Severity

This rule is considered an ERROR since it indicates an invalid file format or file corruption.

Cause

This problem is typically caused by the authoring system that created the image.

Solution

Contact Eclipse Customer Support. The image may need to be re-authored.

Type:	Blu-ray
Reference:	Blu-ray Disc Read-Only Format Part 3: Audio Visual Basic Specifications Version 2.1 Amendments, 12 December 2007
Default Program Action:	Error

Rule ID: 1600

Online certificate revocation list verification error

The digital signature for the online certificate revocation list file is invalid.

Background

The Online certificate revocation list file (online.crl) is one of the components used for certification of network connections by BD-J applications. This file is present only when a BD image includes BD-J applications and it is stored in the \CERTIFICATE folder. During analysis of an image, the online certificate revocation list file is analyzed and its signature is validated.

Online Certificate Revocation List File (online.crl)

Field Name		Description
type_indicator		= "OCRL", identifies the file as an online certificate revocation list file.
version_number		="0200", identifies the online certificate revocation list file version.
reserved		= 00h
Online_CRL	Online_CRL_Version	= '0', identifies the certificate version.
	Number_of_Revocation	Number of revoked content owner's ID records. Each record includes the following fields.
	Revoked_contnet_ownder_ID	The content owner ID value in the revoked online certificate.
	Revocation_type	= 00 00h, indicating 'online certificate revocation'
	Revocation_date	The revocation data as the elapsed date since January 01, 2008. The value 0x0001 = January 01, 2008, 0x0002 = January 02, 2008, etc.
	Online_CRL_Signature	Digital signature of the fields from the start of the online certificate revocation list file to the byte just before the Online_CRL_Signature field, signed by BDA-CA.
	Padding	= 00h

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display more details.

Invalid '[*ContentOwner*]' revocation list. Version [*VersionNo*]. Revocations [*NumberOfRevocations*]

This message shows some of the contents of the certificate revocation list file.

Severity

This rule is considered an ERROR since it indicates a bad file format or file corruption.

Cause

This problem is typically caused by the authoring system that created the image.

Solution

Contact Eclipse Customer Support. The image may need to be re-authored.

Type:	Blu-ray
Reference:	Blu-ray Disc Read-Only Format Part 3: Audio Visual Basic Specifications Version 2.1 Amendments, 12 December 2007
Default Program Action:	Error

Rule ID: 1599

Online certificate verification error

The certificate signature for the online certificate is invalid.

Background

The Online certificate file (online.crt) is one of the components used for certification of network connections by BD-J applications when making network connections. This file is present only when a BD image includes and BD-J applications and it is stored in the \CERTIFICATE folder. During analysis of an image, the online certificate file is analyzed and its signature is validated.

Online Certificate File (online.crt)

Field Name	Description	
type_indicator	="OCRT", identifies the file as an online certificate file	
version_number	="0200", identifies the online certificate file version.	
reserved	=00h	
Online Certificate	Certificate_version	="0", identifies the certificate version
	Content_owner_ID	Unique identifier of the online certificate issued by BDA-CA.
	Reserved	00h
	Content_owner_name	Identifies the content owner as registered in BDA-CA.
	Content_owner_public_key	Identifies the content owner's public key issued by BDA-CA.
	Certificate_signature	Digital signature of the fields from the start of the online certificate through Content_owner_public_key, signed by BDA-CA.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will identify the content owner.

Invalid '[*ContentOwnerName*]' certificate data for network connection

This message identifies the content owner as registered in BDA-CA.

Severity

This rule is considered an ERROR since it indicates a corrupt online certificate file. Without a correct online certificate file the user may not be able to run certain BD-J applications.

Cause

This problem is caused by the authoring system that created the image.

Solution

Contact Eclipse Customer Support for further assistance. It is likely that the image may need to be re-authored.

Type:	Blu-ray
Reference:	Blu-ray Disc Read-Only Format Part 3: Audio Visual Basic Specifications Version 2.1 Amendments, 12 December 2007

Default Program Action: Error

Rule ID: 1589

Online Signature

This is an informational message that identifies the presence of a valid signature in the online signature file (online.sig).

Background

The Online Signature file (online.sig) is one of the components used for certification of network connections by BD-J applications. This file is present only when a BD image includes BD-J applications and it is stored in the \CERTIFICATE folder. During analysis of an image, the online signature file is analyzed and its signature is validated.

Online Signature File (online.sig)

Field Name	Description
type_indicator	= "OSIG", identifies the file as an online signature file.
version_number	= "0200", identifies the online signature file version.
Reserved	= 00h
Online Signature	Digital Signature

Type: Blu-ray

Reference: Blu-ray Disc Read-Only Format
Part 3: Audio Visual Basic Specifications Version 2.1
Amendments, 12 December 2007

Default Program Action: Info

Rule ID: 1596

Online signature file error

One of the fields in the online signature file contains invalid data.

Background

The Online Signature file (online.sig) is one of the components used for certification of network connections by BD-J applications. This file is present only when a BD image includes BD-J applications and it is stored in the \CERTIFICATE folder. During analysis of an image, the online signature file is analyzed and its signature is validated.

Online Signature File (online.sig)

Field Name	Description
type_indicator	= "OSIG", identifies the file as an online signature file.
version_number	= "0200", identifies the online signature file version.

Reserved	= 00h
Online Signature	Digital Signature

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will indicate the cause of this error with one of the following messages.

Type_indicator field is not 'OSIG'

The signature file must begin with the value 'OSIG' identifying the file as an online signature file.

Version_number field is not '0200'

The online signature file must be version '0200'.

Reserved field is not all zeros

All reserved fields must be filled with zeros (00h). However, this condition is not serious since all BD players should ignore reserved fields.

Severity

This rule is considered an ERROR since it indicates an invalid file format. Without a correct signature file, BD-J applications may not function properly.

Cause

This problem is caused by the authoring system that created the image.

Solution

Contact Eclipse Customer Support. The image may need to be re-authored.

Type:	Blu-ray
Reference:	Blu-ray Disc Read-Only Format Part 3: Audio Visual Basic Specifications Version 2.1 Amendments, 12 December 2007
Default Program Action:	Error

Rule ID: 1597

Online signature verification error

The digital signature for the online certificate is not valid.

Background

The Online Signature file (online.sig) is one of the components used for certification of network connections by BD-J applications when making network connections. This file is present only when a BD image includes and BD-J applications and it is stored in the \CERTIFICATE folder. During analysis of an image, the online signature file is analyzed and its signature is validated.

Online Signature File (online.sig)

Field Name	Description
type_indicator	= "OSIG", identifies the file as an online signature file.
version_number	= "0200", identifies the online signature file version.
Reserved	= 00h
Online Signature	Digital Signature

Additional Info

When this rule is triggered, the Additional Info column in the Analysis will display more details about this error.

Invalid '[*ContentOwner*]' app.discroot.crt file

This condition indicates that the file 'app.discroot.crt' file is invalid since the digital signature is based on the contents of this file.

Severity

This condition is considered an ERROR since it indicated a bad file format or file corruption.

Cause

This problem is typically caused by the authoring system that created the image.

Solution

Contact Eclipse Customer Support for further assistance. It is likely that the image may need to be re-authored.

Type:	Blu-ray
Reference:	Blu-ray Disc Read-Only Format Part 3: Audio Visual Basic Specifications Version 2.1 Amendments, 12 December 2007
Default Program Action:	Error

Rule ID: 1591

PAC Content Error

An error occurred while reading the PAC information or a PAC contained invalid information.

Background

Physical Access Control (PAC) Clusters are recorded in the lead-in of a Blu-ray disc to provide additional information for interchange between interchange parties. It is recorded in the INFO1/PAC1 Zone and a backup copy in the INFO2/PAC2 Zone. On a single layer disc, there are 32 Clusters for the storage of PAC information. On a dual-layer disc, there are 64 Clusters. Each Cluster consists of 32 Data Frames.

The EclipseSuite tools read and analyze the information stored in the PAC Clusters. Any non-conformance to the specifications triggers this error.

The layout of a PAC Cluster is as follows:

General Layout of PAC Clusters

Data Frame	Byte Position in Data Frame	Description	Length
0	0	PACK_ID	3
0	3	PACK Format	1
0	4	PAC Update Count	4
0	8	Unknown PAC Rules	4
0	12	Unknown PAC Entire_Disc_Flags	1
0	13	Rserved (=00h)	2
0	15	Number of Segments	1
0	16	Segment 0	8
0	24	Segment 1	8
0	32	:	29 * 8
0	264	Segment 31	8
0	272	Reserved (=00h)	112
0	284	Known PAC Entire_Disc_Flags	1
0	385	Reserved (=00h)	3
0	388	PAC Specific Information	1660
1	0	PAC Specific Information	2048
:	:	:	:
30	0	PAC Specific Information	2048
31	0	Reserved (=00h)	2048

Additional Info

When this error is triggered, the Additional Info column in the analysis will display one of the following messages with more details about the specific cause of this error.

Unable to read PAC from disc

An error occurred when reading the PAC information from a Blu-ray disc. This may indicate a physical error when trying to read from a disc.

Pac Cluster layer [*LayerNo*] failed

An error occurred when reading the PAC information from a Blu-ray disc. This may indicate a physical problem on the media, drive error or corrupt PAC data.

Layer [*LayerNo*] cluster [*ClusterNo*] contained data, but INFO1/PAC1 flags were not set

The Status bits of INFO1/PAC1 location on L0 and Status bits of INFO1/PAC1 locations on L1 are each a 32-bit number, where each bit represents a Cluster location (one bit for each Cluster in the INFO/PAC zones). These bits indicate *whether a location contains a valid PAC. If valid, the related bit is set to 1 or if the location contains all 00h data, then the related bit is set to 0.*

This message indicates valid data was found in a Cluster but the Cluster's status bit indicated that there was no valid data.

Layer [*LayerNo*] cluster [*ClusterNo*] contained data, but INFO2/PAC2 flags were not set

The Status bits of INFO2/PAC2 location on L0 and Status bits of INFO2/PAC2 locations on L1 are each a 32-bit number, where each bit represents a Cluster location (one bit for each Cluster in the INFO/PAC zones). These bits indicate whether a location contains a valid PAC. If valid, the related bit is set to 1 or if the location contains all 00h data, then the related bit is set to 0.

This message indicates valid data was found in a Cluster but the Cluster's status bit was set to 0 indicating that there was no valid data.

Layer [*LayerNo*] cluster [*ClusterNo*] zero data, but INFO1/PAC1 flags were set

The Status bits of INFO1/PAC1 location on L0 and Status bits of INFO1/PAC1 locations on L1 are each a 32-bit number, where each bit represents a Cluster location (one bit for each Cluster in the INFO/PAC zones). These bits indicate whether a location contains a valid PAC. If valid, the related bit is set to 1 or if the location contains all 00h data, then the related bit is set to 0.

This message indicates no valid data was found in a Cluster but the Cluster's status bit was set to 1 indicating that the Cluster contains valid data.

Layer [*LayerNo*] cluster [*ClusterNo*] zero data, but INFO2/PAC2 flags not set

The Status bits of INFO2/PAC2 location on L0 and Status bits of INFO2/PAC2 locations on L1 are each a 32-bit number, where each bit represents a Cluster location (one bit for each Cluster in the INFO/PAC zones). These bits indicate whether a location contains a valid PAC. If valid, the related bit is set to 1 or if the location contains all 00h data, then the related bit is set to 0.

This message indicates no valid data was found in a Cluster but the Cluster's status bit was set to 1 indicating that the Cluster contains valid data.

Layer [*LayerNo*] cluster [*ClusterNo*] NO DATA, but INFO1/PAC1 flags were set

This message indicates that the EclipseSuite tools did not find any data in a Cluster. However, the Status bits of INFO1/PAC1 flags were set indicating that valid data is present.

Layer [*LayerNo*] cluster [*ClusterNo*] NO DATA, but INFO2/PAC2 flags not set

This message indicates that the EclipseSuite tools did not find any data in a Cluster. However, the Status bits of INFO2/PAC2 flags were set indicating that valid data is present.

Layer 0 Primary PAC ID not set to 'PRM'

The first PAC Cluster in the INFO1/PAC1 and INFO2/PAC2 zones is the Primary PAC and must be identified with a PAC_ID value of 'PRM'.

Layer [*LayerNo*] Primary PAC Format (*PACFormat*) expected 0

The PAC Format is used to specify the version of a PAC. In case of the Primary PAC, the PAC Format must be set to 00h indicating Primary PAC version 0.

Layer [*LayerNo*] Primary PAC Update Count ([*Val0*] [*Val1*] [*Val2*] [*Val3*]) expected (00 00 00 00)

The PAC Update Count specifies the total number of update operations of a PAC. For read-only discs, this field must be set to 00 00 00 00h.

Layer [*LayerNo*] Primary PAC Unknown Rules ([*Val0*] [*Val1*] [*Val2*] [*Val3*]) expected (00 AA AA EA)

The Unknown PAC Rules specify the actions to be taken when a PAC is unknown (PAC ID is not set to a known value). In this case, however, this message was triggered on the Primary PAC (PAC ID = 'PRM') and the value for the PAC Unknown Rules must be 00 AA AA EAh.

Layer [*LayerNo*] Primary PAC Unk Entire Disc Flags ([*Re-Init Val*]) expected 1

The Entire Disc Flags byte specifies Unknown PAC Rules that cover the entire disc. Bit 0 (Re-initialization) must be set to 1b indicating that re-initialization of a disc is not possible. All other bits are reserved and must be set to 0b.

Layer [*LayerNo*] Primary PAC Reserved field 1 contains data

The Primary PAC header includes reserved fields all of which must be set to 00h. This message indicates that the first reserved field contains non-zero data.

Layer [*LayerNo*] Primary PAC Number of Segments ([*NumberOfSegments*]), Expected 0

The Number Of Segments field in a PAC specify the total number of segments specified in the current PAC. In a Primary PAC, this field must be set to 00h.

Layer [*LayerNo*] Primary PAC Segment [*SegmentNo*] Start ([*Val0*] [*Val1*] [*Val2*] [*Val3*]) expected (00 00 00 00)

The first four bytes of a Segment field contain the first physical sector number of the first Cluster belonging to the Segment. The last four bytes contain the last physical sector number of the last Cluster belonging to the Segment. However, this message is triggered for the Primary PAC, which must have these bytes set to 00h.

Layer [*LayerNo*] Primary PAC Segment [*SegmentNo*] end ([*Val0*] [*Val1*] [*Val2*] [*Val3*]) expected (00 00 00 00)

The first four bytes of a Segment field contain the first physical sector number of the first Cluster belonging to the Segment. The last four bytes contain the last physical sector number of the last Cluster belonging to the Segment. However, this message is triggered for the Primary PAC, which must have these bytes set to 00h.

Layer [*LayerNo*] Primary PAC reserved area 2 contains data

The Primary PAC header includes reserved fields all of which must be set to 00h. This message indicates that the second reserved field contains non-zero data.

Layer [*LayerNo*] Primary PAC Known PAC Entire Disc Flags ([*Re-Init Val*]) expected 1

The Known PAC Entire Disc Flags byte specifies known PAC Rules that cover the entire disc. Bit 0 (Re-initialization) must be set to 1b indicating that re-initialization of a disc is not possible. All other bits are reserved and must be set to 0b.

Layer [*LayerNo*] Primary PAC Reserved area 3 contains data

The Primary PAC header includes reserved fields all of which must be set to 00h. This message indicates that the third reserved field contains non-zero data.

Layer [*LayerNo*] Primary PAC INFO1/PAC1 L0 location bits ([*Val0*] [*Val1*] [*Val2*] [*Val3*]), expected at least one cluster (80 00 00 00)

The Status bits of INFO2/PAC2 location on L0 and Status bits of INFO2/PAC2 locations on L1 are each a 32-bit number, where each bit represents a Cluster location (one bit for each Cluster in the INFO/PAC zones). These bits indicate whether a location contains a valid PAC. If valid, the related bit is set to 1 or if the location contains all 00h data, then the related bit is set to 0.

Since there must be at least the Primary PAC, it is expected that at least one Cluster be tagged as valid. Since currently only the Primary PAC is defined, it is expected that the Status bits of the INFO1/PAC1 be set to 80 00 00 00h.

Layer [*LayerNo*] Primary PAC INFO2/PAC2 L0 location bits ([*Val0*] [*Val1*] [*Val2*] [*Val3*]), expected at least one cluster (80 00 00 00)

The Status bits of INFO2/PAC2 location on L0 and Status bits of INFO2/PAC2 locations on L1 are each a 32-bit number, where each bit represents a Cluster location (one bit for each Cluster in the INFO/PAC zones). These bits indicate whether a location contains a valid PAC. If valid, the related bit is set to 1 or if the location contains all 00h data, then the related bit is set to 0.

Since there must be at least the Primary PAC, it is expected that at least one Cluster be tagged as valid. Since currently only the Primary PAC is defined, it is expected that the Status bits of the INFO2/PAC2 be set to 80 00 00 00h.

Layer [*layerNo*] Primary PAC reserved area at end of sector contains data

The Primary PAC header includes reserved fields all of which must be set to 00h. This message indicates that bytes 404 ~ 2047 of the Primary Cluster contains non-zero data. These bytes have not been defined and must be set to 00h.

PAC Frame [*FrameNo*] contains data (PRM invalid)

Currently, only Data Frame 0 is defined by the specifications. All other Data Frames are reserved and must be set to 00h.

This message is triggered when checking the contents of the Data Frames in a Cluster.

Severity

This rule is considered an ERROR since some of the conditions listed above indicate a failure to read the PAC data. It is possible that this may lead to playability problems.

Cause

When this error is triggered on a BDCMF image, the problem may be caused by the utility that created the PAC information. However, if this occurs on a disc, it may also be caused by a hardware failure or physical defect on the media.

Solution

If the problem occurs on a BDCMF image, then the image must be re-authored with the correct PAC information. If the problem occurs on a disc, then test on multiple players to see if the problem follows the media or player.

Type:	Blu-ray
Reference:	Blu-ray Disc Read-Only Format Part 1: Basic Format Specifications Version 1.3
Default Program Action:	Error

Rule ID: 1428

PAL compatible video frame-rate

The EclipseSuite tools detected a video stream with a video frame rate of 25MHz or 50MHz, which may present some problems during playback on some Blu-ray players.

Background

This rule is triggered when the EclipseSuite tools detect video streams with MPEG-2, MPEG-4 or VC-1 video codec and video frame rates of 25Hz or 50Hz. Support for these frame rates is only mandatory in countries that use a 50Hz TV system (PAL). In all other countries, the 25/50Hz frame rate support is optional.

The specifications recommends authors to run an initial application to determine if that disc will be playable when authoring an image with only 25/50Hz content. If the player does not support the frame rate, then a message should be displayed to the user. Similarly, BD-ROM Player manufacturers are also encouraged, but not required, to display a message when playing back a 25/50Hz AV stream file and the BD Player does not support it.

Unfortunately, there are images containing 25/50Hz content that are authored in a way that does not check player compatibility with the disc's video frame rate. Similarly, there are BD players that don't check for compatibility and/or warn the user. The result can lead to playability problems such as a blank screen.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis may display more details.

'[*PlayList*]', PI([*PlayItem#*]) S([*PrimaryVideoStreamEntry#*]), [*VideoStreamCodingType*] [*VideoFormat*] [*FrameRate*]

This message can be used to identify where this condition was triggered:

- ***PlayList*** - *the PlayList file where this condition was detected (e.g. 00000.mpls).*
- ***PlayItem#*** - *a numeric ID of the PlayItem where this condition was detected.*
- ***PrimaryVideoStreamEntry#*** - *a numeric ID of the Primary Video Stream that triggered this condition.*
- ***VideoStreamCodingType*** - *identifies the video codec as MPEG2, MPEG4 or VC-1.*
- ***VideoFormat*** - *identifies the video format as 480i, 576i, 480p, 1080, 720p, 1080p or 576p.*
- ***FrameRate*** - *identifies the video frame rate as 23.976Hz, 24Hz, 25Hz, 29.97Hz, 50Hz or 59.94Hz.*

A PlayList (.mpls) has references to PlayItems. PlayItems have references to a section of a Clip AV stream files (*.m2ts), which contain the audio/video information. The PlayItem also includes video attributes describing the audio/video information referenced by the PlayItem.*

Severity

25/50Hz frame rates support is required in countries using the PAL TV system. There have been reports of playability problems when they are used. The problem reports were specific to Sony players, including the PS3. Since these are valid frame rates, this rule defaults to INFO severity.

Cause

This rule created to identify Blu-ray images that use 25Hz or 50Hz video frame rates. It does not necessarily ndicate a problem with an image since these frame rates are supported by the specifications.

Solution

It is highly recommended that playability tests are performed on the final replicas, especially on Sony and PS3 BD players.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Info

Rule ID: 1627

Partial BDCMF missing CPS Unit Key file

The Plain CPS Unit Key File is not specified in the BDCMF.CMF file.

Background

Blu-ray images with partial Info (Type AX), require the file UKF.DAT. This file is a copy of the Unit_Key_RO.inf from a Type C1 or Type C2 image. The purpose of this file is to be included with the original Type A image and be sent back to the original customer for archiving. If in the future the customer wants the image re-mastered, customer can use the original AACS encryption files (including UKF.DAT) to process the image.

Severity

This condition indicates a problem with the BDCMF.CMF file. The entry that describes the UKF.DAT file is present but the filename is not. It is unknown how programs that will process the image will react to this error. It is possible that programs will automatically look for this file by name since the naming convention is fixed and as long as the file is present there may not be any problems. However, it is unknown if all systems will do the same. Therefore, this condition is considered an ERROR.

Cause

This problem is caused by the utility that modified the BDCMF.CMF file and created the entry for the UKF.DAT file. In most cases, this will be the utility that encrypted the image (for example ImageCopy).

Solution

The solution depends on where in the process this error got introduced. Contact Eclipse Support for assistance.

Type:	Blu-ray
Reference:	BDCMF Specifications
Default Program Action:	Error

Rule ID: 1654

Partial BDCMF missing Order Delivery file

The reference to the order delivery file in the BDCMF file is missing the order delivery filename.

Background

A BDCMF image with Partial Info (Type AX) must include all the necessary files to be able to re-master without having to re-submit anything to AACS LA. This means that the original order delivery file must be present. The BDCMF file in this type of image includes references to some of these files. This rule indicates that the reference to the order delivery file is missing the filename.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will identify the layer for which this rule is triggered.

Severity

The order delivery file is required in order to process this image. Therefore, this condition is considered an ERROR.

Cause

This problem may be caused by the utility that created the Type AX image.

Solution

The original order delivery file must be located. Otherwise, the image must be processed as though it has never been mastered before. Contact Eclipse Support for further assistance.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Warning

Rule ID: 1655

Philips RMI License expiration notice

This rule is used to alert the user that the Philips RMI License is about to expire.

Background

The Philips RMI license must be renewed every 3 months. The Philips RMI License software alerts the user prior to expiring. The alert message can be configured to appear when a specified number of counts are left in the License.

Please contact Philips for License renewal information.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Warning

Rule ID: 1558

PIC BCA Flag Comparison Error

The BCA Flag in the BDCMF.CMF file is different from the BCA Flag in the PIC.DAT file.

Background

The BCA Flag indicates whether the final disc will include a BCA. BCA is used to serialize discs to support online transactions. This flag also determines whether a BCA band will be recorded on each disc after replication. If the BCA Flag in the PIC data is enabled but no BCA is recorded, then some players may fail.

Additional Info

When this rule is triggered, the Additional Info column in the Analysis will display the BCA Flag values it found.

Severity

Since this condition has the potential for causing playability problems, this is considered an ERROR.

Cause

This condition is normally caused by the authoring system that created the image. However, it can also happen if an image requiring a BCA is authored correctly but the BCA is not recorded.

Solution

A solution to this problem depends on the condition that caused it. Please contact Eclipse support for further assistance.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

Rule ID: 1676

PIC Comparison Error

The PIC data between the source and target images do not match.

Background

PIC data (Permanent Information and Control data) describes physical characteristics of a Blu-ray disc. This is similar to the Control data information on a DVD. PIC data is recorded in the PIC zone in the lead-in. It consists of a PIC Info Fragment which is repeated five times. Each PIC Info Fragment consists of 848 Physical Clusters.

Data Frame 0 of the first Physical Cluster of each Info Fragment contains the Disc Information Block. Data Frame 30 of the first Physical Cluster of each Info Fragment contains Emergency Break data.

The Disc Information Block consists of up to 32 Disc Information Units (DI Units). Each layer must include the same number of DI Blocks with the same DI units.

To protect against possible drive & media combinations, the Blu-ray specifications define the Emergency Break that can be used by specific drive models to recognize discs that need special handling to prevent fatal errors.

When comparing two Blu-ray images, the DI Units and Emergency Break data items are compared between the source and target. If any item does not match, then this rule is triggered.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will identify the specific field within the DI Unit or Emergency Break data that triggered this rule.

Disc Information Unit

Byte	Field Name	Description
0	Disc Information Identifier	= "DI" (44h 49h), Identifies this structure as a DI Unit.
2	DI Number	= 01h, Identifies the contents of the DI Unit. This may vary depending on the layer type.
3	Number of DI Units	specifies the number of DI Units in each DI Block = 00001b for SL discs = 00010b for DL discs
	Layer number	Specifies the layer number to which this DI Unit applies = 000b for byte 3 on SL/DL disc indicating layer 0 = 001b for byte 67 on DL disc indicating layer 1
4	Reserved	= 00h
5	DI Unit sequence number	Specifies the sequential DI Unit number within the DI Block = 00h for SL discs = 00h and 01h sequentially for DL discs
6	Continuation flag	Specifies if the parameters of this DI Unit is continued in the next DI Unit = 0b indicating the next DI Unit is the start of a new set of parameters = 1b indicating the parameters of this DI unit are continued in the next DI Unit
	Number of DI bytes in use	= 20h indicating that only the first 32 bytes of the DI Unit are used. All others are reserved.
7	Reserved	= 00h
8 to 10	BD Layer Type identifier	= "BDO", identifies the type of BD layer to which this DI Unit applies
11	Disc Size	= 00b indicating a 120mm disc = 01b indicating an 80mm disc
	Class	= 00b
	Version	= 0001b indicating a layer according to the BD Read-Only specifications.
12	BD Structure	Specifies the number and type of recording/recorded layers
	Total Number of Layers	= 0001b indicating 1 recorded layer (SL discs) = 0010b indicating 2 recorded layers (DS discs
	Type of Recorded Layer	= 00001b indicating a read-only recorder layer
13	Hybrid Disc Identifier	Bits b7 to b4 indicate the presence of DVD or CD layers. = 0000b for BD discs according to the Read-Only specifications.
	Channel bit length	Bits b3 to b0 specify the main data channel bit length. = 0000b reserved = 0001b indicating a channel bit length of 74.5 nm (25GB max per layer) = 0010b indicating a channel bit length of 69.0 nm (27GB max per layer) Others, reserved

14	Push-Pull polarity flag bits	Each bit b_i specifies the polarity of the Push-Pull signal on Recorded layer i. = 0b indicating that the Push-Pull polarity on Layer i is positive. = 1b indicating that the Push-Pull polarity on Layer i is negative. For recording layers that are not present, bit b_i is set to 0b.
15	Reserved	= 00h
16	BCA descriptor	= 0000b for bits b7 to b4 Bits b3 to b0 indicate the presence of a BCA-code on the disc = 0000b indicate no BCA = 0001b indicate that BCA is present
17	Maximum transfer rate	= 00h indicating no maximum transfer rate is specified
18 to 19	Reserved	= 00h
20 to 23	Last User Data Address	Specifies the physical sector number of the physical sector contains the last user data.
24 to 31	Data Zone allocation	Specifies the first and last Address Unit Number of the Data Zone of the related layer.
	First AUN	Bytes 24 to 27 specify the first AUN of the Data Zone = 00 10 00 00h for each DI Unit related to layer 0. For DI Units relating to layer 1: ≥ 01 35 8C 00h for a disc with a Channel bit length of 74.5 nm ≥ 01 26 AF 40h for a disc with a Channel bit length of 69.0 nm
	Last AUN	Bytes 28 to 31 specify the last AUN of the Data Zone For DI Units relating to layer 0: ≤ 00 CA 73 FEh for a disc with a Channel bit length of 74.5 nm ≤ 00 D9 50 BEh for a disc with a Channel bit length of 69.0 nm For each DI Unit relating to layer 1: = 01 EF FF FEh
32 to 60	Reserved	= 00h
61 to 62	Timestamp	Optional timestamp indicating the production date of the master disc.
63	Reserved	= 00h

Refer to the picture above for the following messages.

Source layers ([*NumLayers*]), target ([*NumLayers*])

The number of layers specified in the Disc Structure byte does not match between the source and target. Bits 4-7 of the Disc Structure byte specify the total number of BD Recording/Recorded Layers on a disc. On a Single Layer disc, these bits must be set to 0001, indicating 1 Recorded Layer. On a Dual Layer disc, these bits must be set to 0010, indicating 2 Recorded Layers.

Layer [*LayerNum*] DiscInfo identifier, Source ('[*Byte#0*] [*Byte#1*]'), Target ('[*Byte#0*] [*Byte#1*]')

Bytes 0 and 1 identify the Disc Information structure with the values 44 49h, representing the characters "DI". These are the only valid values for these bytes.

Layer [*LayerNum*] DI Format number, Source ([*DIFormatNumber*]), Target ([*DIFormatNumber*])

While each Layer Type can have its own independent DI Format Number, a read-only Layer must have a DI Format Number value of 01h.

Layer [*LayerNum*] dual number DI units, Source ([*NumDIUnits*]), Target ([*NumDIUnits*])

The Number of DI Units in each DI Block must be a number between 1 and 32, inclusive. On a read-only single layer disc, the number of DI Units is 1 (00001b). On a dual-layer read-only disc, the number of DI Units is 2 (00010b). This is specified with bits 3-7 in byte 3 of a DI Unit.

Layer [*LayerNum*] reserved field 1, Source (Resvd1), Target (Resvd1)

Byte 4 is reserved and must be set to 00h.

Layer [*LayerNum*] DI unit sequence number, Source ([*DIUnitSeqNo*]), Target ([*DIUnitSeqNo*])

A DI Block may include up to 32 DI Units. The Sequence Number specifies the sequential DI Unit number within the DI Block. On a single layer disc, the sequence number must be set to 00h. On a dual layer disc, it must be set to 00h and 01h. The DI Unit with sequence number 00h should have the parameters for layer 0, while the DI Unit with sequence number 01h should have the parameters for layer 1.

Layer [*LayerNum*] Number of DI bytes, Source ([*NumDIBytes*]), Target ([*NumDIBytes*])

Bits 0-6 of byte 6 indicate the number of bytes in use in the DI Unit. Currently only the first 32 bytes are used. Therefore, these bits must have the value 20h indicating that only the first 32 bytes of the DI Unit are used.

Layer [*LayerNum*] reserved field 2, Source ([*Resvd2*]), Target ([*Resvd2*])

Byte 7 is reserved and must be set to 00h.

Layer [*LayerNum*] disc type, Source ([*DiscType*]), Target ([*DiscType*])

Bytes 8-10 identify the type of BD layer to which this DI Unit applies and must be set to the value 42 44 4Fh, representing the characters "BDO". This must be set in each read-only layer.

Layer [*LayerNum*] disc version, Source ([*DiscVer*]), Target ([*DiscVer*])

Bits 0-3 of byte 11 specify the Version number. These bits must be set to 0001, indicating a layer according to the Blu-ray Basic Format Specifications v1.3.

Layer [*LayerNum*] disc class, Source([*DiscClass*]), Target ([*DiscClass*])

Bits 4-5 of byte 11 specify the Class number. The Class number is used to identify BD layers of the same Layer Type but with different basic specifications such as higher data densities. Discs according to the BD Read-Only specifications must have these bits set to 00.

Layer [*LayerNum*] disc size, Source ([*DiscSize*]), Target ([*DiscSize*])

Bits 6-7 of byte 11 specify the disc size. These must be set to 00, indicating a 120 mm disc or 01, indicating an 80 mm disc.

Layer [*LayerNum*] disc layer type, Source ([*LayerType*]), Target ([*LayerType*])

Bits 0-3 of byte 12 (BD Structure) specify the Layer Type to which this DI Unit applies. On discs according to the BD Read-Only specifications, these bits must be set to 0001, indicating a Read-Only Recording Layer.

Layer [*LayerNum*] number of layers, Source ([*NumLayers*]) Target ([*NumLayers*])

Bits 4-7 of byte 12 (BD Structure) specify the total number of BD Recording/Recorded Layers in the disc. On a single layer disc, these bits must be set to 0001, indicating 1 Recorded Layer. On a dual layer disc, these bits must be set to 0010, indicating 2 Recorded Layers.

Layer [*LayerNum*] channel bit rate flag, Source ([*MainDataChannelBit*]), Target ([*MainDataChannelBit*])

Bits 0-3 of byte 13 specify the Channel bit length, which must be the same on all BD Recorded layers. These bits must have the following values:

0000 = indicates a channel bit length of 80.0nm (23.3 GB / layer)
0001 = indicates a channel bit length of 74.5nm (25.0 GB / layer)
0010 = indicates a channel bit length of 69.0nm (27.0 GB / layer)
Others = Reserved.

Layer [*LayerNum*] hybrid CD flags, Source ([*CDHybridFlags*]), Target ([*CDHybridFlags*])

Bits 4-5 of byte 13 are used to indicate the presence of a CD layer on a BD disc. These bits must be set to one of the following values:

00 = No CD layer present
01 = CD read-only layer(s)
10 = CD recordable layer(s)
11 = CD rewritable layer(s)

Layer [*LayerNum*] hybrid DVD flags, Source ([*DVDHybridFlags*]), Target ([*DVDHybridFlags*])

Bits 6-7 of byte 13 are used to indicate the presence of a DVD layer on a BD disc. These bits must be set to one of the following values:

00 = No DVD layer present
01 = DVD read-only layer(s)
10 = DVD recordable layer(s)
11 = DVD rewritable layer(s)

Layer [*LayerNum*] Push/Pull Polarity Flags, Source ([*PushPullPolarityFlags*]), Target ([*PushPullPolarityFlags*])

Each bit in byte 14 represent a layer. Each bit also specifies the polarity of the Push-Pull signal on the Recorded Layer represented by the bit. The bits must be set as follows:

0 = indicating that the Push-Pull polarity on the Layer is positive.
1 = indicating that the Push-Pull polarity on the layer is negative.
Recording layers that are not present, the bits representing those layers must be set to 0.

Layer [*LayerNum*] reserved field, Source ([*Resvd3*]), Target ([*Resvd3*])

Byte 15 is reserved and must be set to 00h.

Layer [*LayerNum*] BCA flag does, Source ([*BCAPresent*]), Target ([*BCAPresent*])

Bits 0-3 of byte 16 indicate the presence of a BCA code on the disc. These bits must be set to one of the following values:

- *0000 = No BCA code*
- *0001 = BCA code present*
- *Others = Reserved*

Layer [*LayerNum*] reserved 4 field, Source ([*Resvd4*]), Target ([*Resvd4*])

Bits 4-7 of byte 16 are reserved and must be set to 0000.

Layer [*LayerNum*] Max Transfer Rate, Source ([*MaxTransferRate*]), Target ([*MaxTransferRate*])

Byte 17 specifies the maximum read transfer rate (Mbit/s) needed by the application. This byte must be set to 00h, indicating that no maximum transfer rate is specified.

Layer [*LayerNum*] Reserved field, Source (*Resvd5*), Target(*Resvd5*)

Bytes 18 & 19 are reserved and must be set to 00h.

layer [*LayerNum*] reserved field 6

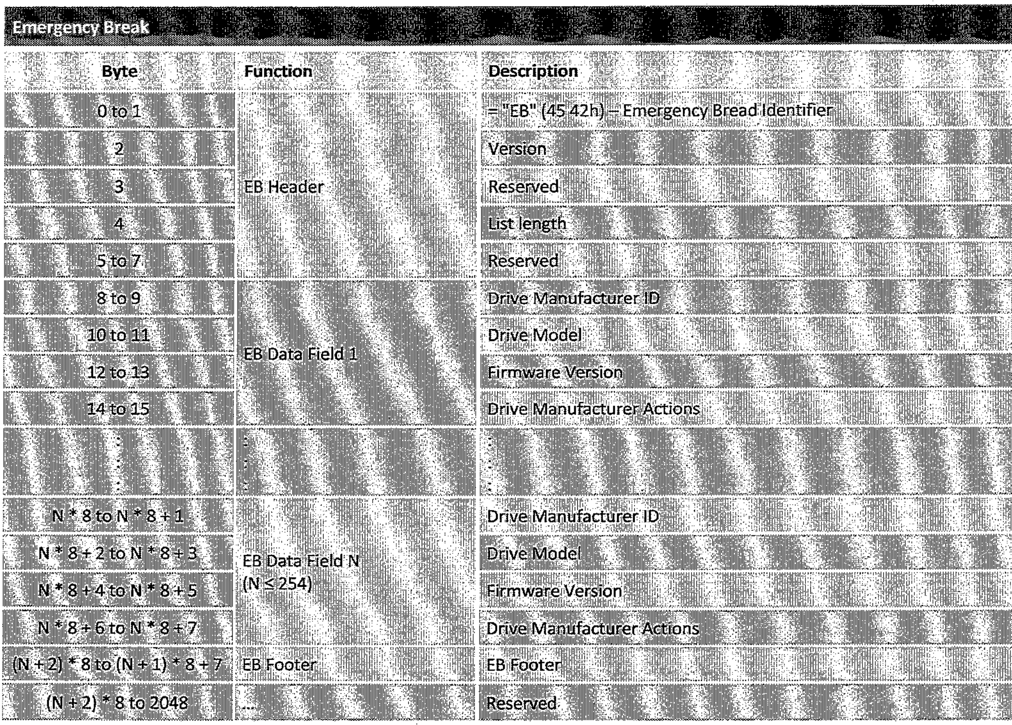
All reserved bytes in a DI Unit must be set to 00h. In a DI Unit, only the first 32 bytes are used. This message is displayed when bytes 32 to 60 are not set to 00h.

layer [*LayerNum*] reserved field 7, Source ([*Resvd7*]), Target ([*Resvd7*])

Byte 63 is reserved and must be set to 00h.

Emergency Brake Header, Source ([*EB ID*]), Target ([*EB ID*])

Bytes 0 and 1 of the Emergency Break header must be set to 45 42h, representing the characters "EB" for the identification o Emergency Break data.



Emergency Break

Byte	Function	Description
0 to 1	EB Header	= "EB" (45 42h) – Emergency Bread Identifier
2		Version
3		Reserved
4		List length
5 to 7		Reserved
8 to 9	EB Data Field 1	Drive Manufacturer ID
10 to 11		Drive Model
12 to 13		Firmware Version
14 to 15		Drive Manufacturer Actions
:	:	:
N * 8 to N * 8 + 1	EB Data Field N (N ≤ 254)	Drive Manufacturer ID
N * 8 + 2 to N * 8 + 3		Drive Model
N * 8 + 4 to N * 8 + 5		Firmware Version
N * 8 + 6 to N * 8 + 7		Drive Manufacturer Actions
(N + 2) * 8 to (N + 1) * 8 + 7	EB Footer	EB Footer
(N + 2) * 8 to 2048	...	Reserved

Refer to the picture above for the following messages.

mergency Brake Header version, Source ([*Version*]), Target ([*Version*])

yte 2 of the Emergency Break header must be set to 01h, representing Version 1 of the Emergency Break format.

mergency Brake Header Reserved field 1, Source ([*Reserved*]), Target ([*Reserved*])

yte 3 is reserved and must be set to 00h.

mergency Brake Header List Length, Source ([*Length*]), Target ([*Length*])

yte 4 represents the number of EB data fields. There can be a maximum of 255 (0 to 254). The value must be specified in exadecimal format.

mergency Brake Header Reserved field 2

ytes 5-7 are reserved and must be set to 00h.

ype:	Blu-ray
eference:	System Description Blu-ray Disc Read-Only Format Part 1: Basic Format Specifications Version 1.3
efault Program Action:	Error

ule ID: 1475

IC Content Error

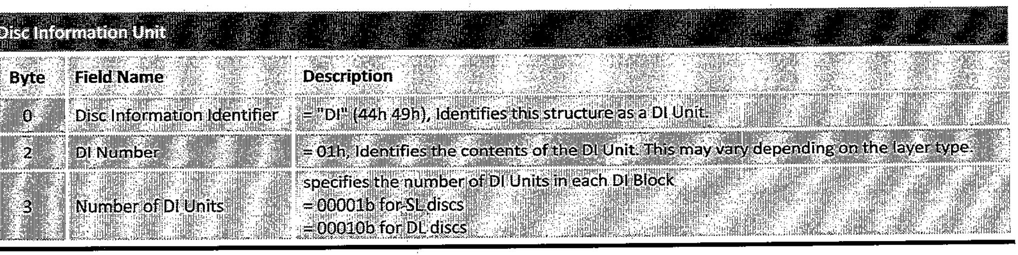
he data in the PIC Zone of the Blu-ray disc is invalid.

ackground

IC data refers a zone within the lead-in area used for the recording of various types of data such as Disc nformation. The Disc Information includes properties to describe a BD disc. This is similar to the Control ata information of a DVD disc.

he Disc Information Block is divided into 64-byte Disc Information (DI) Units. There can be a maximum f 32 DI Units. However, currently, only one DI Unit is required to describe a Single Layer disc and two DI nits are required to describe a Dual-Layer disc. The first DI Unit describes Layer 0 (or single layer) and the econd DI Unit describes Layer 1.

uring the analysis of the media, the EclipseSuite tools read the PIC data and verify its contents. Since this ule is triggered for any error in the PIC data, the Additional Info column is used to indicate the specific eld within the PIC data that caused the error.



isc Information Unit

Byte	Field Name	Description
0	Disc Information Identifier	= "DI" (44h 49h), Identifies this structure as a DI Unit.
2	DI Number	= 01h, Identifies the contents of the DI Unit. This may vary depending on the layer type.
3	Number of DI Units	specifies the number of DI Units in each DI Block = 00001b for SL discs = 00010b for DL discs

	Layer number	Specifies the layer number to which this DI Unit applies = 000b for byte 3 on SL/DL disc indicating layer 0 = 001b for byte 67 on DL disc indicating layer 1
4	Reserved	= 00h
5	DI Unit sequence number	Specifies the sequential DI Unit number within the DI Block = 00h for SL discs = 00h and 01h sequentially for DL discs
6	Continuation flag	Specifies if the parameters of this DI Unit is continued in the next DI Unit = 0b indicating the next DI Unit is the start of a new set of parameters = 1b indicating the parameters of this DI unit are continued in the next DI Unit
	Number of DI bytes in use	= 20h indicating that only the first 32 bytes of the DI Unit are used. All others are reserved.
7	Reserved	= 00h
8 to 10	BD Layer Type identifier	= "BDO", identifies the type of BD layer to which this DI Unit applies
11	Disc Size	= 00b indicating a 120mm disc = 01b indicating an 80mm disc
	Class	= 00b
	Version	= 0001b indicating a layer according to the BD Read-Only specifications.
12	BD Structure	Specifies the number and type of recording/recorded layers
	Total Number of Layers	= 0001b indicating 1 recorded layer (SL discs) = 0010b indicating 2 recorded layers (DS discs
	Type of Recorded Layer	= 00001b indicating a read-only recorder layer
13	Hybrid Disc Identifier	Bits b7 to b4 indicate the presence of DVD or CD layers. = 0000b for BD discs according to the Read-Only specifications.
	Channel bit length	Bits b3 to b0 specify the main data channel bit length. = 0000b reserved = 0001b indicating a channel bit length of 74.5 nm (25GB max per layer) = 0010b indicating a channel bit length of 69.0 nm (27GB max per layer) Others, reserved
14	Push-Pull polarity flag bits	Each bit b_i specifies the polarity of the Push-Pull signal on Recorded layer i. = 0b indicating that the Push-Pull polarity on Layer i is positive. = 1b indicating that the Push-Pull polarity on Layer i is negative. For recording layers that are not present, bit b_i is set to 0b.
15	Reserved	= 00h
16	BCA descriptor	= 0000b for bits b7 to b4 Bits b3 to b0 indicate the presence of a BCA-code on the disc = 0000b indicate no BCA = 0001b indicate that BCA is present
17	Maximum transfer rate	= 00h indicating no maximum transfer rate is specified
18 to 19	Reserved	= 00h
20 to 23	Last User Data Address	Specifies the physical sector number of the physical sector contains the last user data.
24 to 31	Data Zone allocation	Specifies the first and last Address Unit Number of the Data Zone of the related layer.
	First AUN	Bytes 24 to 27 specify the first AUN of the Data Zone = 00 10 00 00h for each DI Unit related to layer 0. For DI Units relating to layer 1: ≥ 01 35 8C 00h for a disc with a Channel bit length of 74.5 nm ≥ 01 26 AF 40h for a disc with a Channel bit length of 69.0 nm

	Last AUN	Bytes 28 to 31 specify the last AUN of the Data Zone For DI Units relating to layer 0: ≤ 00 CA 73 FEh for a disc with a Channel bit length of 74.5 nm ≤ 00 D9 50 BEh for a disc with a Channel bit length of 69.0 nm For each DI Unit relating to layer 1: = 01 EF FF FEh
32 to 60	Reserved	= 00h
61 to 62	Timestamp	Optional timestamp indicating the production date of the master disc.
63	Reserved	= 00h

Additional Info

When this error occurs, the **Additional Info** column in the Analysis will display more specific details about the condition that triggered the error.

Layer 1 PIC Data not found

This message indicates that the disc is a Dual-Layer Blu-ray disc and that the DI Unit that describes Layer 1 was not found within the PIC data that was read from the disc.

As of version 1.3 of the Blu-ray Disc Read-Only Format specifications, a maximum of two DI Units are required to describe a BD disc; one for Layer 0 (or single layer) and one for Layer 1. On a dual layer disc, the second DI Unit should contain the information describing Layer 1. The EclipseSuite tools read all DI Units and could not find one describing Layer 1.

Layer 1 PIC Data found at SHIFTED offset [*offset*]

The PIC data for Layer 1 is expected at the second DU Unit (byte offset 64) of the Disc Information Block.

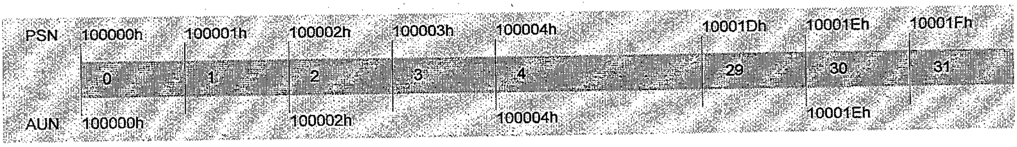
As of Version 1.3 of the Blu-ray Disc Read-Only Format specifications, only two DI Units are required to describe a Blu-ray disc; one DI Unit for Layer 0 (or single layer) and one for Layer 1.

This message indicates that there were additional DI Units and that the DI Unit that describes Layer 1 was found at a later DI Unit.

PIC Last User PSN ([*last User PSN*]) must be Last AUN ([*last AUN*]) + 1

The last Physical Sector Number (PSN) of user data on Layer 0 must be equal to the last Address Unit Number (AUN) in Layer 0 + 1.

The Physical Sector Numbers increment sequentially from 0 to the end of each layer. The Address Unit Numbers, on the other hand, increment by 2 from 0 to the end of each layer. Physical Sector Numbers are Virtual Physical Sectors since they are not actually recorded on the media. They are used to address individual user data sectors.
Address Unit Numbers is used to address blocks (cluster) of 32 user data sectors. Since the length of the user data area must be a multiple of 32 user data sectors, the last PSN on layer 0 will be equal to the last AUN + 1.



PIC L1 Last AUN ([*last AUN*]) incorrect

Since the track pitch, velocity, start and end radii are all pre-defined in the specifications, the number of sectors that will fit in the user data area of layer 1 is a fixed value. On layer 1, the last AUN must always be equal to 1EFFFFFEh and the last PSN is 1EFFFFFFh (last AUN + 1).

Rom Mark flag mismatch: PIC flag: ([*enabled/disabled*]), CMF Flag ([*enabled/disabled*])

The CPS_Sector in the PIC data contains a flag that indicates whether or not a BD image will require a ROM-Mark. On a BDCMF image, the PIC data is stored in the PIC.DAT file. The ROM-Mark flag (RMF) is stored in bit 7 of byte 0 of the CPS_Sector.
RMF = 0/1

Similarly, a BD image using BDCMF 0.92 or later includes a flag in the BDCMF.CMF file that also indicates whether a ROM-Mark needs to be recorded.

ROM-Mark="USE"

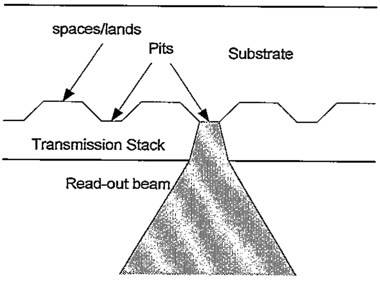
This message indicates that the ROM-Mark flag in the PIC.DAT file does not match with the ROM-Mark flag in the BDCMF.CMF file.

Rom Mark Flag Missing

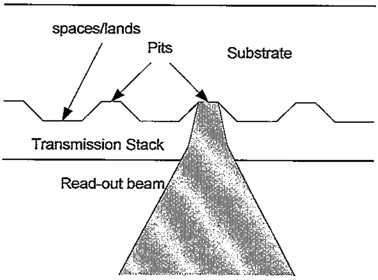
This message indicates that the ROM-Mark flag in the CP_Sector is not specified or the version of BDCMF is less than 0.92.

Layer 0 Push/Pull Pol. flag actual [*FlagValue*], expected 0-3

The Push-Pull flag polarity bits are used to indicate whether a layer is recorded using "On-Pit recording" or "In-Pit recording". This is also known as positive polarity or negative polarity.



"On-Pit recording"

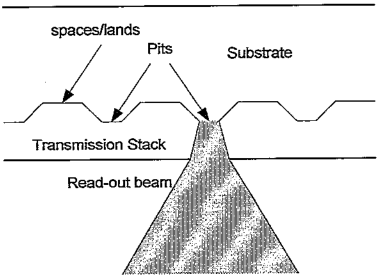


"In-Pit recording"

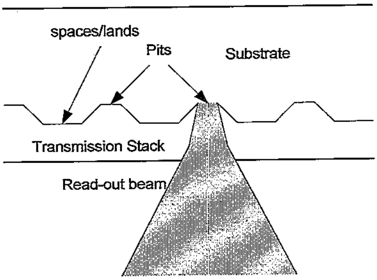
The BDCMF specifications require these flag bits to be set to 01h for single layer images and 03h for dual layer images. These values indicate negative polarity ("In-Pit recording"). The EclipseSuite tools check the value of the flag bits to make sure that they are between 00h and 03h. If any other value is found, then this message is displayed.

Layer 1 Push/Pull Pol. flag actual [*FlagValue*], expected 0-3

The Push-Pull flag polarity bits are used to indicate whether a layer is recorded using "On-Pit recording" or "In-Pit recording". This is also known as positive polarity or negative polarity.



"On-Pit recording"



"In-Pit recording"

The BDCMF specifications require these flag bits to be set to 01h for single layer images and 03h for dual layer images. These values indicate negative polarity ("In-Pit recording"). The EclipseSuite tools check the value of the flag bits to make sure that they are between 00h and 03h. If any other value is found, then this message is displayed.

layer [*LayerNo*] DiscInfo identifier incorrect - expected 'DI'

Every DI Unit starts with a two-byte identifier, which must be set to the characters 'DI'.

Layer [*LayerNo*] DI Format number incorrect ([*FormatNo*])

The Format number identifies the contents of a DI Unit. On a read-only layer, this value must be set to 01h.

Layer [*LayerNo*] dual layer number DI units incorrect ([*NumberOfDIUnits*])

This message indicates an incorrect number of DI units based on the number of layers. A single layer image requires 1 DI Unit, while a dual-layer requires 2 DI Units.

single layer number DI units incorrect ([*NumberOfDIUnits*])

This message indicates that there are 2 DI Units but the image is single layer. A single layer image should only have 1 DI Unit.

Number of DI units ([*NumberOfDIUnits*]) incorrect for [*NumberOfLayers*] layers

This message indicates that there are less than 1 DI Units or more than 2. Since Blu-ray images are either single or dual-layer, the number of DI Units should be 1 or 2, respectively.

Layer [*LayerNo*] reserved field 1 contains data

All reserved fields in the DI Unit must be set to 00h data. This message indicates that non-zero data was found.

Layer [*LayerNo*] DI unit sequence number [*SequenceNo*], expected [*ExpectedValue*]

The Sequence Number specifies the sequential DI Unit number within the DI Block. On single layer images, this must be set to 00h. On a dual-layer image, this must be set to 00h and 01 sequentially. The DI Unit with Sequence number 00h contains the information for layer 0 and the DI Unit with Sequence number 01h contains the information for layer 1.

Layer [*LayerNo*] Number of DI bytes incorrect ([*NumberOfDIBytes*]) expected (32)

The bits representing the Number of DI bytes should have a value of 20h (32), indicating that the first 32 bytes of the DI Unit are used. All remaining bytes of the DI Unit are reserved.

Layer [*LayerNo*] reserved field 2 contains data

All reserved fields in the DI Unit must be set to 00h data. This message indicates that non-zero data was found.

Layer [*LayerNo*] incorrect disc type specified

The Layer Type field in a DI Unit identifies the layer type. All read-only layers must have a value of "BDO", which identifie a read-only layer.

Layer [*LayerNo*] disc class set incorrectly

The Class bits identify BD layers of the same Layer Type but with different specifications, such as different data densities. Read-only layers must have these bits set to 00b.

Layer [*LayerNo*] disc version not set to 1

The Version bits must be set to 0001b, indicating that a layer is recorded according to the Blu-ray read-only specifications.

Layer [*LayerNo*] disc layer type not set to 1

The Layer Type bits in the BD Structure field of a DI Unit specify the type of recording/recorded layer on a disc. When describing a read-only layer, these bits must be set to 0001b.

Layer [*LayerNo*] number of layers ([*ActualNumberOfLayers*]) expected ([*ExpectedNumberOfLayers*])

The Number of Recording/Recorded Layers in the BD Structure field of a DI Unit specify the total number of BD Recording/Recorded layer on the disc. These bits must be set to 0001b for single layer, indicating 1 recorded layer and 0010b for dual-layer discs, indicating 2 recorded layers.

Layer [*LayerNo*] only channel bit rate of 74.5nm allowed

The Channel Bit Length bits specify the main data channel bit length on a BD recorded layer. Currently, the only correct value is 0001b, indicating a channel bit length of 74.5 nm (25.0 GB max. per layer).

Hybrid CD Flag ([*HybridFlagValue*]) incorrect - expected (01)

The Hybrid Disc bits (bits 5 to 4) are used to indicate the presence of CD or DVD layers on the disc. This message indicates that a read-only CD layer is recorded but the CD flag bits indicate a no CD layer is recorded or that the CD layer is recordable or rewritable. Currently, only read-only CD layers are expected.

00b = no CD layer present
01b = CD read-only layer(s) present
10b = CD recordable layer(s) present
11b = CD rewritable layer(s) present

Hybrid DVD Flag ([*HybridFlagValue*]) incorrect - expected (01)

The Hybrid Disc bits (bits 7 to 6) are used to indicate the presence of CD or DVD layers on the disc. This message indicates that a read-only CD layer is recorded but the CD flag bits indicate a no CD layer is recorded or that the CD layer is recordable or rewritable. Currently, only read-only CD layers are expected.

00b = no DVD layer present
01b = DVD read-only layer(s) present
10b = DVD recordable layer(s) present
11b = DVD rewritable layer(s) present

Layer [*LayerNo*] reserved field 3 contains data

All reserved fields in the DI Unit must be set to 00h data. This message indicates that non-zero data was found.

Layer [*LayerNo*] BCA flag does not match PMSN setting

When the BCA flag bits are set (0001b = BCA is present), the PMSN must also be set. If BCA is not present, then PMSN must not be present either. PMSN is a Prerecorded Media Serial Number, which is recorded within the BCA.

Layer [*LayerNo*] reserved 4 field contains data

All reserved fields in the DI Unit must be set to 00h data. This message indicates that non-zero data was found.

Layer [*LayerNo*] Max Transfer Rate [*ActualMaxTransferRate*], expected 0

The Maximum Transfer Rate field must be set to 00h, indicating that no maximum transfer rate is specified.

Layer [*LayerNo*] Reserved field 5 contains data

All reserved fields in the DI Unit must be set to 00h data. This message indicates that non-zero data was found.

Layer [*LayerNo*] reserved field 6 contains data

All reserved fields in the DI Unit must be set to 00h data. This message indicates that non-zero data was found.

Layer [*LayerNo*] reserved field 7 contains data

All reserved fields in the DI Unit must be set to 00h data. This message indicates that non-zero data was found.

Emergency Break

Byte	Function	Description
0 to 1	EB Header	= "EB" (45 42h) – Emergency Bread Identifier
2		Version
3		Reserved
4		List length
5 to 7		Reserved
8 to 9	EB Data Field 1	Drive Manufacturer ID
10 to 11		Drive Model
12 to 13		Firmware Version
14 to 15		Drive Manufacturer Actions
: : :	: : :	: : :
N * 8 to N * 8 + 1	EB Data Field N (N ≤ 254)	Drive Manufacturer ID
N * 8 + 2 to N * 8 + 3		Drive Model
N * 8 + 4 to N * 8 + 5		Firmware Version
N * 8 + 6 to N * 8 + 7		Drive Manufacturer Actions
(N + 2) * 8 to (N + 1) * 8 + 7	EB Footer	EB Footer

(N + 2) * 8 to 2048	...	Reserved

Refer to the table above for the remaining conditions.

Emergency Brake Header not set to 'EB'

The Emergency Break is identified in the first two bytes by the characters 'EB'.

Emergency Brake Header version [*ActualVersion*], expected 1

The Emergency Break version must be set to 1.

Emergency Brake Header Reserved field 1 contains data

All reserved fields in the Emergency Break must be set to 00h data. This message indicates that non-zero data was found.

Emergency Brake Header Reserved field 2 contains data

All reserved fields in the Emergency Break must be set to 00h data. This message indicates that non-zero data was found.

Severity

Since the above conditions indicate errors in the physical parameters of the media, this rule is considered an ERROR. However, there may be some fields that may not be considered as an error, such as the non-zero reserved fields.

Cause

This problem is caused by the authoring system that created the image.

Solution

The image must be re-authored.

Type:	MainChannel
Reference:	Blu-ray Disc Read-Only Format Part 1: Basic Format Specifications Sections: 6.3.1.1.1 & 6.3.1.1.2
Default Program Action:	Error

Rule ID: 860

PIC data & CMF image sector count disagree

The last sector of user data specified in the PIC data does not agree with the BDCMF image size.

Background

On a BDCMF image, the size of the image is specified in the BDCMF.CMF file and in the PIC data file. During analysis, the EclipseSuite tools compare the size in these two locations. If they do not match then this error occurs.

The field "Last User Data Address" in the PIC data zone in the lead-in specifies that last user data sector. The BDCMF file has a **<File ... >** XML element which describes the user data file (UD.DAT). In it there is an attribute which specifies the image length.

Using Last User Data Address information from the PIC data, the length can be calculated by subtracting its value from the starting address where the user data is recorded (100000h), then adding 1.

LastUserDataAddress - 100000h + 1 = Length

In the BDCMF.CMF file, the image length is specified by a File element as shown in the sample below.

```
...
<ImageData>
    <File Type="PICData" Name="PIC.DAT" Size="65536">
      <HashValue HashType="SHA-1">1234123412341234123412341234123412341234</HashValue>
    </File>
    <File Type="PACDataLayer0" Name="PACL0.DAT" Size="65536">
      <HashValue HashType="SHA-1">4123412341234123412341234123412341234123</HashValue>
    </File>
    <File Type="UserControlData" Name="UCD.DAT" Size="75857472">
      <StartPSN>00100000</StartPSN>
      <HashValue HashType="SHA-1">3412341234123412341234123412341234123412</HashValue>
    </File>
    <File Type="UserData" Name="UD.DAT" Size="8630894592">
      <StartPSN>00100000</StartPSN>
      <HashValue HashType="SHA-1">2341234123412341234123412341234123412341</HashValue>
    </File>
</ImageData>
...
```

Additional Info

When this rule is triggered, the Additional Info column in the Analysis will display the differences between the PIC data and BDCMF.CMF file with one of the following messages.

PIC Last User Address:(*LastUserDataAddress*), CMF (*TotalSectors*)

The calculated length using the PIC data Last User Data Address does not match the length specified in the BDCMF.CMF file.

PIC Last AUN (*LastAUN*) > Layer 0 size (*TotalSectors*)

The last Address Unit Number (AUN) must be equal to or less than the image length. If it is less, then it must be within 32 sectors of the image length.

Type:	Blu-ray
Reference:	BDCMF Specifications System Description Blu-ray Read-Only Format Part 1: Basic Format Specifications Section 6.3.1 Permanent Information & Control Data (PIC) Zone
Default Program Action:	Error

Rule ID: 857

Placeholder Title component not as recommended

The explanation for this title check rule contains confidential information. Please refer to the studio-specific supplemental rules help PDF document. The document is available from Eclipse Support.

Type: Blu-ray
Reference: N/A
Default Program Action: Warning

Rule ID: 1675

PlayList file structural error

The EclipseSuite tools detected errors while analyzing a PlayList file.

Background

Part of the analysis of a Blu-ray Video image includes analysis of the contents of PlayList files. PlayList files contain references to PlayItems, which contain references to segments of AV data in a Clip AV Stream file. If during this analysis, the EclipseSuite tools find any errors then this rule is triggered.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display the condition that triggered it with one of the following messages

PlayItem (#), failed to initialize primary video stream (#) in PlayList file '[PlayListFilename]'
PlayItem (#), failed to initialize primary audio stream (#) in PlayList file '[PlayListFilename]'
PlayItem (#), failed to initialize PG textST stream (#) in PlayList file '[PlayListFilename]'
PlayItem (#), failed to initialize IG stream (#) in PlayList file '[PlayListFilename]'
PlayItem (#), failed to initialize secondary audio stream (#) in PlayList file '[PlayListFilename]'
PlayItem (#), failed to initialize secondary video stream (#) in PlayList file '[PlayListFilename]'
ext_data_entry (#), failed to initialize STN_table_SS() PlayItem (#), primary_video_stream (#) in PlayList file '[PlayListFilename]'
ext_data_entry (#), failed to initialize STN_table_SS() PlayItem (#), PG_textST_stream (#) base view in PlayList file '[PlayListFilename]'
ext_data_entry (#), failed to initialize STN_table_SS() PlayItem (#), PG_textST_stream (#) dependent view in PlayList file '[PlayListFilename]'
ext_data_entry (#), failed to initialize STN_table_SS() PlayItem (#), PG_textST_stream (#) top AS in PlayList file '[PlayListFilename]'
ext_data_entry (#), failed to initialize STN_table_SS() PlayItem (#), PG_textST_stream (#) bottom AS in PlayList file '[PlayListFilename]'
ext_data_entry (#), failed to initialize STN_table_SS() PlayItem (#), IG_stream (#) base view in PlayList file '[PlayListFilename]'
ext_data_entry (#), failed to initialize STN_table_SS() PlayItem (#), IG_stream (#) dependent view in PlayList file '[PlayListFilename]'
Missing PlayItem (#) for ext_data_entry (#), SubPath_block_extension() SubPath (#) type 8
Missing PlayItem (#), Angle (#) for ext_data_entry (#), SubPath_block_extension() SubPath (#) type 8
Invalid memory access

Severity

All of the conditions listed above are considered serious and, therefore, this rule is an ERROR.

Cause

This condition is caused by the authoring system that created the image.

Solution

The image must be re-authored. Contact Eclipse Customer Support for further assistance.

Type:	Blu-ray
Reference:	Blu-ray Video Specifications
Default Program Action:	Error

Rule ID: 1758

Pre-encrypted HDMV stream

The Blu-ray image includes pre-encrypted data.

Background

The BDCMF specifications classify BDCMF images in 'Types' based on their data type content type and protection status. This error occurs when analyzing a Type A image and the EclipseSuite tools find that Clip files have been encrypted. Type A images are not supposed include any encrypted content. During encryption, a Type A image is taken as input and results in a Type B encrypted image in the output. The original Type A image is not changed.

During the analysis, the EclipseSuite tools detect this condition and will not re-encrypt the content. However, the EclipseSuite tools need to identify the CPS Unit Key that was used to encrypt the content. If this is not possible, then other errors will follow.

Additional Info

When this rule is triggered, the **Additional Info** column will identify the Clip file that has been pre-encrypted.

Severity

Since a Type A image is not supposed to be encrypted, this condition is considered an ERROR. This will likely cause the EclipseSuite tools to trigger other errors and abort the job.

Cause

Since a Type A image is typically the output of an authoring system, it is assumed that the authoring system is the cause of this problem.

Solution

The image should be re-authored.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

Rule ID: 1575

Process goal

This is an informational message that displays the BDCMF Type that ImageCopy will output.

Background

BDCMF 0.97 supports several image Types. Depending on the source BDCMF, ImageCopy may output a different BDCMF image Type.

Type:	Other
Reference:	BDCMF Specifications
Default Program Action:	Info

Rule ID: 1530

Producer Application ID mismatch

The explanation for this title check rule contains confidential information. Please refer to the studio-specific supplemental rules help PDF document. The document is available from Eclipse Support.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

Rule ID: 1669

Producer Organization ID mismatch

The explanation for this title check rule contains confidential information. Please refer to the studio-specific supplemental rules help PDF document. The document is available from Eclipse Support.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

Rule ID: 1652

Push Pull Polarity Flag overridden

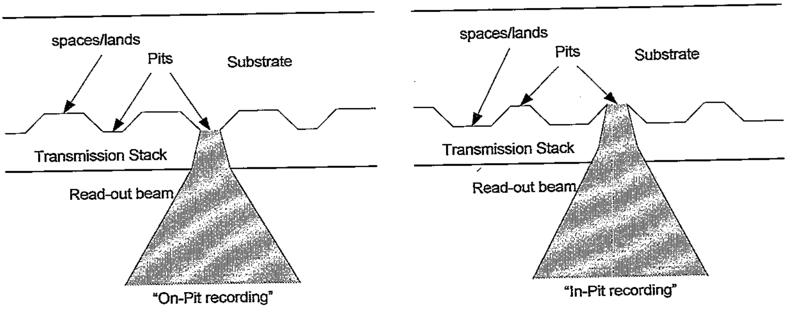
This ImageEncoder rule indicates that the BD Push Pull polarity flag has been overridden.

Background

The Push Pull bits describe the pit geometry on a disc. Traditionally, a pit is recorded when the laser is turned on. Blu-ray supports another method that is the opposite. The Blu-ray specifications define the Pit Geometry as follows:

On a Blu-ray disc, both "On-Pit recording" and "In-Pit recording" are allowed. On-Pit recording is a method where the pits are closer to the Entrance surface of the disc than the Spaces/Lands. In-Pit recording is a method where the pits are farther from the Entrance surface of the disc than the

Spaces/Lands.



The pit geometry is specified in the PIC data during lead-in. However, in the ImageEncoder, this can be overridden via a registry setting. When overridden, this rule is triggered to notify the user.

Type:	Blu-ray
Reference:	Blu-ray Disc Read Only Format Part 1: Basic Format Specifications Section 6.3.1
Default Program Action:	Flag

Rule ID: 1499

Removing public key from recipients, matching private key missing

A public key is being removed since there is no matching private key present.

Background

On a BDCMF Type B and C, the user data has been encrypted and the encryption keys are stored in a file within the image itself. The file containing the encryption keys does not get encrypted until the mastering process. This means that on a Type B and C image, the encryption keys are not protected. BDCMF 1.10 includes the ability to protect the encryption keys during the encryption process of the image. The output image is referred to as a 'Secure BDCMF' Type BS and CS (the 'S' indicates Secure).

On a Secure BDCMF image, the original source image is encrypted as usual. However, rather than storing the encryption keys in the image, they are stored in a separate file called KEY.DAT. This file can further be encrypted to protect its contents. ImageCopy can encrypt this file by using a SmartCard. A SmartCard contains a private and public key. When the encrypted image is processed later, the same SmartCard is required. If the image is to be processed in different computers, then each computer requires a SmartCard. Furthermore, the public key of each computer that is to process the image needs to be imported into the certificate store of the computer that is doing the encryption.

This rule indicates that a Secure BDCMF image is being processed with ImageCopy or ImageEncoder. The KEY.DAT file was encrypted with more than one public key. However, the local computer does not include a copy of each of the public keys that were used to encrypt it. Therefore, ImageCopy will encrypt the KEY.DAT of the output image using only the public keys that are in the local computer. If the source image was encrypted using other public keys that don't exist in the local computer, then they will be 'removed'.

Additional Info

When this rule is triggered, the Additional Info column in the analysis will list the public keys that were removed.

Severity

This rule does not indicate a problem with the image. However, it does indicate that the image may not be able to be processed on certain computers. Therefore, this rule defaults to a WARNING.

Cause

This rule is triggered when ImageCopy is processing a Secure BDCM image and the local computer does not have a matching list of public keys to which the KEY.DAT was encrypted.

Solution

Nothing needs to be done unless the image requires to be processed on the computer for which the public key was removed.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Warning

Rule ID: 1844

Replaced UDF file

This rule indicates that a file has been replaced while processing the image. Normally, file replacing occurs in Blu-ray images. This condition does not indicate a problem. Therefore, its severity is only a Flag.

Type:	Verification
Reference:	N/A
Default Program Action:	Flag

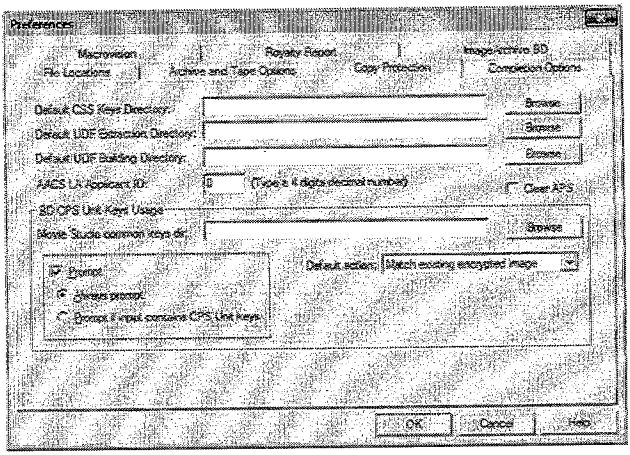
Rule ID: 1707

Reusing CPS Unit Key

ImageCopy will be re-using a CPS Unit Key from another image for the encryption of the current image.

Background

By default, ImageCopy automatically generates new keys during the encryption of an image. However, ImageCopy allows the user to specify alternate CPS Unit Keys via the ImageCopy Preferences (File | Preferences | Copy Protection).



Default CSS Keys Directory:

Default UDF Extraction Directory:

Default UDF Building Directory:

AACS LA Applicant ID: 0 (Type a 4 digits decimal number)

☐ Clear APS

BD CPS Unit Keys Usage

Movie Studio common keys dir:

☑ Prompt

● Always prompt

○ Prompt if input contains CPS Unit keys

Default action: Match existing encrypted image

- **Generate new** – This is the default. Using this option causes ImageCopy to automatically generate CPS Unit Keys for encryption of the user data.
- **Preserve embedded values** -- By default, the file in the image where the CPS Unit Keys are stored is empty (i.e. filled with zeros). During encryption, ImageCopy generates the CPS Unit Keys and stores them in this file. However, during authoring, it is possible for the author to include CPS Unit Keys in this file. If the existing CPS Unit Keys are to be used, then the user must select this option so that ImageCopy uses the existing keys instead of generating new ones.
- **Match existing encrypted image** – Selecting this option allows the user to direct ImageCopy to use CPS Unit Keys from an already-encrypted image. This is useful when an image must be re-encrypted.
- **Preserve keys found in external file** -- Using this option allows the user to specify an external file (MKB_RO.inf) where ImageCopy can get the CPS Unit Keys instead of generating new ones. The file must be in the local folder from where the EclipseSuite tools are run. It is also assumed that the file includes enough CPS Unit Keys.

Severity

This rule indicates that a CPS Unit Key is being re-used to encrypt the current image. It is not a violation of the specifications. It is provided for informational purposes only.

Cause

This rule is triggered when the user has selected **"Preserve embedded values"**, **"Match existing encrypted image"** or **"Preserve keys found in external file"** from the ImageCopy Copy Protection Preferences.

Solution

This rule is included for informational purposes only. It does not indicate a problem.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Info

Rule ID: 1569

ROM Mark

This rule is used to indicate that information has been sent to the ROM Mark Inserter unit successfully.

Background

All Blu-ray titles require a ROM Mark. The ROM Mark is placed on the image during mastering in a special process. This process requires a ROM Mark Inserter from Eclipse, Sony or Phillips. This message appears in the analysis of the ImageEncoder program to identify that the information required by the ROM Mark Inserter was received and processed. If there are problems with this transfer then a ROM Mark Send Error message will be displayed with further details on the problem.

Additional Info

When this rule is triggered, the **Additional Info** column in the analysis will display the following message indicating that the data required by the ROM Mark Inserter has been sent, received and verified OK.

Process Completed

This message indicates that the ROM Mark data has been sent to the ROM Mark Inserter, received and verified OK. This message is triggered for the Philips RMI and Sony RIU2000 systems.

Data Written to File [FileName]

This message indicates that the ROM Mark data has been sent to the ROM Mark Inserter, received and verified OK. Additionally, the KCD and VID were written to an external file as specified by the system configuration. This message is triggered for the Philips RMI system.

Process completed via DCHK

This message indicates that the ROM Mark data has been sent to the ROM Mark Inserter, received and verified OK. This message is triggered for the Eclipse RMU-7000 system.

Data sent to external application

This message indicates that the ROM Mark data has been sent to the ROM Mark Inserter, received and verified OK. This message is triggered for the Eclipse RMU-7000 and Sony RIU2000 systems.

Type:	Exclude
Reference:	N/A
Default Program Action:	Info

Rule ID: 861

ROM Mark Send Failure

An error occurred when sending the Rom Mark information to the RMI Unit.

Background

When mastering a Blu-ray image, the Eclipse ImageEncoder communicates with Sony's RMI unit and exchanges information with it. This rule is triggered if any problems occur during this process.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display one of the following messages providing more details.

Could not create communication interface

This message is displayed when the ImageEncoder fails to open a communications interface to the RMI unit. Verify that the RMI unit is connected to the ImageEncoder system and that it is properly configured. Contact Eclipse Customer Support for further assistance.

Could not establish communication

This message is displayed when the ImageEncoder fails to establish communication with the RMI unit. Verify that the RMI unit is connected and properly configured. Contact Eclipse Customer Support for further assistance.

Error [*ErrorNo*] attempting to process CMF data

An error occurred while processing CMF data that was to be sent to the RMI unit.

Could not create UDF mounting object

This message is displayed when ImageEncoder is unable to create a UDF mounting object in order to access the contents of the image. This is required when reading and sending image information to be sent to the RMI unit.

Error Reading key values from BDCMF

This message is displayed when ImageEncoder fails to read required keys from the BDCMF image that are required by the RMI unit.

Encryption Key Error

Contact Eclipse Customer Support

COM Port Not Set

This message indicates that the communication port where the RMI unit is connected is not properly setup. Verify that the port is properly setup and contact Eclipse Customer Support for further assistance.

Error sending data

This message indicates an error by the RMI unit when data was sent to it by the ImageEncoder. Contact Eclipse Customer Support for further assistance.

Encryption Error

This message indicates that there was an error encrypting the ROM Mark data. Contact Eclipse Customer Support for further assistance.

Missing KCD or VID

The KCD or VID is required when sending Rom Mark information to the RMI unit. Contact Eclipse Customer Support for further assistance.

Image is not Signed

This message indicates that you are attempting to master an image that has not been signed yet.

Type: Exclude
Reference: N/A
Default Program Action: Error

Rule ID: 881

Rom Mark unit did not return to idle state

This rule is an informational message that lets users know when the state of the Philips ROM Mark Inserter did not return to an idle state. Currently this is not known to be a problem.

Type: Blu-ray
Reference: N/A
Default Program Action: Flag

Rule ID: 1812

Secure BDCMF KEY.DAT file missing

The BDCMF file is missing a reference to the 'KEY.DAT' file.

Background

In BDCMF 1.10, the file 'KEY.DAT' contains highly confidential information for image types BS and CS. Therefore, when creating a Type BS or CS image, the BDCMF.CMF file must include a reference to this file.

The KEY.DAT file is used to store confidential copy protection information. In previous versions of BDCMF, this information was stored with the image. In BDCMF 1.10, this information can be stored in the KEY.DAT file and not on the image. When the image is mastered, the encoder merges it with the image in memory. The KEY.DAT file itself can be encrypted in order to protect its content.

Severity

This rule indicates that the image is Type BS or CS and, therefore, the KEY.DAT file should be present. Without this file, it may not be possible to process this image. Therefore, it is considered an ERROR.

Cause

This error can occur when moving the image without this file. It may be possible that it can occur if processing the image with a version of software that does not support this type of image (Type BS/CS).

Solution

This error indicates that the KEY.DAT file did exist at one point. It may have been removed or left behind in part of normal processing of the image. The file must be located. Otherwise, the complete encryption process may need to be performed again.

Type: Blu-ray
Reference: BDCMF 1.10 Specifications
Default Program Action: Error

Rule ID: 1659

Severe Error encountered

A serious error occurred when processing the Content Certificate (CC) or Content Hash Table (CHT) files.

Background

During processing of a Blu-ray image, the content of the CC and CHT files will be verified and may be modified. This condition may occur if the content of the CC or CHT files is invalid or it may indicate an internal problem with the EclipseSuite applications.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display more information with one of the following messages.

Unable to process Content Hash Table data

A Content Hash Table file for an image that is already encrypted (Type B or later) should include hash entries for the Clip files in the layer that it represents. This message indicates that the EclipseSuite tools did not find any hash entries. However, it may also indicate an internal program error.

Hash and Content Certificate data checks/replacement incomplete

This message indicates that an error occurred when checking or replacing the Content Certificate file. This may also indicate an internal program error.

Severity

This rule indicates a serious problem with the image or an internal problem with the EclipseSuite application.

Cause

While there are rules that test for specific 'known' conditions, this rule is designed to catch unknown conditions that may cause processing of the CC and CHT files to fail. If this rule is triggered, it indicates a serious problem with the image or an internal problem with the EclipseSuite application.

Solution

Contact Eclipse Customer Support for further assistance. It is likely that a log file will be required. Please email the log file to Eclipse Customer Support with your questions.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

Rule ID: 1549

SHA-1 mismatch

The calculated hash value for a BDCMF image file does not match the expected value.

Background

The BDCMF.CMF file includes hash values for each of the files that are part of a BDCMF image. The hash value is stored in the <File> elements of the BDCMF.CMF file as shown in the example below:

```
<ImageData>
  <File Type="PICData" Name="PIC.DAT" Size="65536">
    <HashValue HashType="SHA-1">1234123412341234123412341234123412341234</HashValue>
  </File>
  <File Type="PACDataLayer0" Name="PACL0.DAT" Size="65536">
    <HashValue HashType="SHA-1">4123412341234123412341234123412341234123</HashValue>
  </File>
  <File Type="UserControlData" Name="UCD.DAT" Size="75857472">
    <StartPSN>00100000</StartPSN>
    <HashValue HashType="SHA-1">3412341234123412341234123412341234123412</HashValue>
  </File>
  <File Type="UserData" Name="UD.DAT" Size="8630894592">
    <StartPSN>00100000</StartPSN>
    <HashValue HashType="SHA-1">2341234123412341234123412341234123412341</HashValue>
  </File>
</ImageData>
```

The hash values are like checksums in that they are used to check the integrity of the files. When the image is authored, the authoring system automatically generates a hash value for each of the image files. This rule is triggered when the hash value for one of the files does not match the recalculated value.

Be aware that support for SHA-1 is not available in all versions of EclipseSuite. If an image was processed with an old version of the CMU utility that does not update the SHA-1 value, then this error may occur if the image is later analyzed with a more current version of ImageAnalysis or ImageVerify.

NOTE!
If you have images that trigger this rule because they were processed with a version of the CMU that did not update the SHA-1, you can update the SHA-1 by running ICheck on the image with the ***"Calculate SHA-1 for BDCMF"*** *option selected in the Options menu.*

Additional Info

When this rule is triggered, the **Additional Info** column in the analysis will display more details with the following messages.

File '[*Filename*]'. Expected '[*Expected Hash Value*]'. Actual '[*Actual Hash Value*]'

This message is displayed when the recalculated hash value for one of the image files does not match the hash value specified in the BDCMF.CMF file.

PIC.DAT

When this message identifies the PIC.DAT file, the most likely cause of this problem is that the hash value was not updated by the program that previously modified this file. However, if there is also a "File Checksum error" for the PIC Data file, then it may indicate that the file is corrupt.

When a BDCMF image is authored, the authoring system is required to generate a SHA-1 value for the PIC data file. The SHA-1 is stored in the BDCMF.CMF file. When the image is Signed, the PIC data file is modified and the utility used for Signing the image must update the SHA-1. If the utility that was used to Sign the image does not support SHA-1 or if it fails updating the SHA-1, then it will result in this condition.

It is unusual for this rule to be triggered due to file corruption. This is why it is only considered a WARNING. When it occurs because of file corruption, the error "Bad file checksum" should be triggered for the same file. It is possible that other errors or warnings may be triggered depending on where the corruption occurred in the file.

UD.DAT & UCD.DAT
When the image is encrypted using ImageCopy, the SHA-1 will not be updated since ImageCopy would have to make a second pass on the image to recalculate it. Instead, ImageCopy will remove the old SHA-1 value from the BDCMF file so that it does not cause this rule to be triggered the next time it is analyzed. To check integrity of these files, Eclipse relies on the ImageSignature and file checksums. However, users can update the SHA-1 by running ICheck and selecting "Calculate SHA-1 for BDCMF" from ICheck's Options menu.

Other Files
The rest of the image files are not modified by the Eclipse software. Therefore, if this message identifies any other file, then it indicates possible file corruption.

Severity

The most common cause of this condition is when the SHA-1 value for the PIC.DAT file is not updated after the image is Signed. It does not indicate that the file is corrupt. Therefore, this is only considered a WARNING.

If this rule is triggered together with the error **"Bad file checksum"**, then it indicates that the file is corrupt. In that case, this condition should be considered an ERROR.

Cause

The most common cause for this rule is that the PIC.DAT file is not updated after the image is signed. Although, it is also possible that this can occur if a file becomes corrupt.

Solution

When this rule identifies the PIC.DAT file with the SHA-1 mismatch and not file checksum error occurs, then this rule can be ignored. However, check for any other related errors or warning related to this file.

If this rule identifies any other file, then it may indicate that the file is corrupt. When this happens, there are typically other related errors such as "Bad file checksum" that may follow. In that case, the image must be rejected.

Contact Eclipse Customer Support for further assistance.

Type:	Blu-ray
Reference:	BDCMF
Default Program Action:	Warning

Rule ID: 1538

Signed application requires authentication message

A signed BD-Java application is missing a file that is required for authentication.

Background

BD-Java applications and related files are stored in JAR files inside the JAR directory. The META-INF directory inside a JAR file includes the Manifest, Signature and Signature Block files. The Manifest file includes a hash for each file inside the JAR file. The Signature file has a similar structure as the Manifest file. However, the Signature file includes a hash for each file entry in the Manifest file. It also includes a hash for the whole Manifest file. The Signature file is signed and its signature is stored in a certificate inside the Signature Block file.

The Manifest, Signature and Signature Block files are referred to as 'messages' in BD-Java Security. All three are required when authenticating a signed BD-Java application. Since there can be multiple signers, the Signature and Signature Block files have an identifier in their filename which uniquely identifies each pair.

Signature File: **SIG-BDxx.SF**
Signature Block File: **SIG-BDxx.RSA**

The **xx** portion of the filename is an identifier that starts with '00'. Any additional pairs must have this value incremented by one. The JAR Manifest filename is 'MANIFEST-MF'.

Additional Info

When this error occurs, the **Additional Info** column in the Analysis will display more details with one of the following messages.

'[*BDJOFile*]' [*AppID*], '[*JARFile*]', JAR Manifest File '[*FileName*]'

This condition indicates that the Manifest file (MANIFEST.MF) is missing inside the JAR file. There must be exactly one manifest file in a JAR file and it should be recorded inside the META-INF directory. This message also identifies the BD-J Object file, JAR File and Application ID.

'[*BDJOFile*]' [*AppID*], '[*JARFile*]', Signature Block File '[*SIG-BDxx.RSA*]'

This condition indicates that the Signature Block file (SIG-BDxx.RSA) is missing inside the JAR file. There must be at least one pair of Signature Block file (SIG-BD00.RSA) and a Signature file (SIG-BD00.SF) in a JAR file and they should be recorded inside the META-INF directory. This message also identifies the BD-J Object file, JAR File and Application ID.

'[*BDJOFile*]' [*AppID*], '[*JARFile*]', Signature File '[*SIG-BDxx.SF*]'

This condition indicates that the Signature file (SIG-BDxx.SF) is missing inside the JAR file. There must be at least one pair of Signature Block file (SIG-BD00.RSA) and a Signature file (SIG-BD00.SF) in a JAR file and they should be recorded inside the META-INF directory. This message also identifies the BD-J Object file, JAR File and Application ID.

Severity

If any of the three files mentioned above is missing from the META-INF directory inside a JAR file, then the BD-Java applications and related files inside the JAR file cannot be authenticated. Therefore, this is considered an ERROR.

Cause

This problem typically occurs in authoring of the image.

Solution

The image must be re-authored.

Type: Blu-ray
Reference: Blu-ray Specifications, Section 3-2: BD-Java Specifications
Default Program Action: Error

Rule ID: 1633

Source CC File Hash Data Incorrect

The hash values for certain files inside the Content Certificate file are incorrect.

Background

The Content Hash Table includes a hash value for every hash unit of every Clip AV stream file. The hashes in the Content Hash Table are then hashed and the hash values are stored in the Content Certificate file as digest entries. Additionally, the Content Certificate includes a hash value for the Managed Copy Manifest File, the BD-J Root Certificate file and all CPS Unit Usage files. This rule indicates that the hash values for one or more of these files is incorrect.

Additional Info

When this rule is triggered, the **Additional Info** column in the analysis will identify the file whose hash value is incorrect.

MC Manifest File Hash Data corrected

The existing hash values for the Managed Copy Manifest file (mcmf.xml) do not match the recalculated hash values. The original values will be overwritten.

BD-J root certificate File Hash Data corrected

The original hash values for the Application Root Certificate file (app.discroot.crt) do not match the recalculated values. The original values will be overwritten.

CPSUnitUsage [*CPSUnitUsageFileNo*] File Hash Data corrected (*Layer 0*)

The existing hash values for the CPS Unit Usage file on layer 0 do not match the recalculated values. The original values will be overwritten.

CPSUnitUsage [*CPSUnitUsageFileNo*] File Hash Data corrected (*Layer 1*)

The existing hash values for the CPS Unit Usage file on layer 1 do not match the recalculated values. The original values will be overwritten.

Severity

Since the EclipseSuite tools are able to correct this condition, it is only considered a WARNING.

Cause

This problem is typically caused by the authoring system that created the image.

Solution

If the image is processed with the ImageCopy, the problem should be corrected on the output image. It is strongly recommended that a separate analysis or verification be performed on the output image to confirm.

Type:	MainChannel
Reference:	AACS Specifications
Default Program Action:	Warning

Rule ID: 879

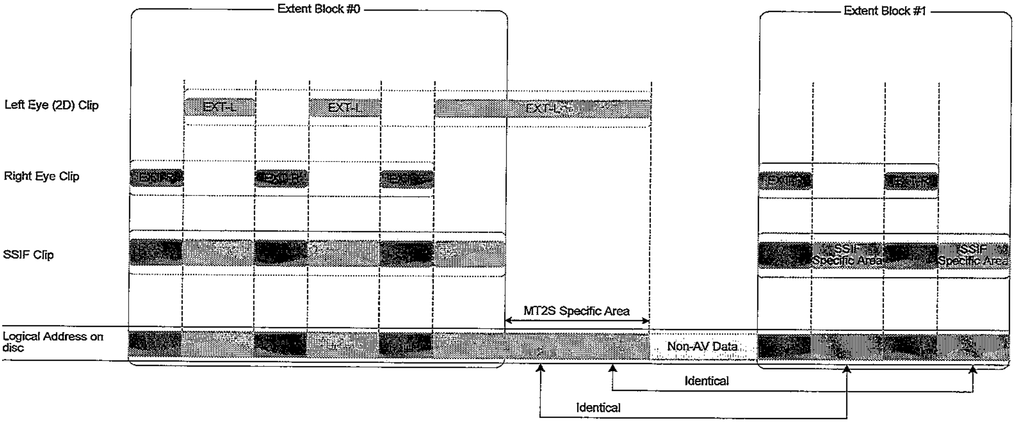
SSIF and M2TS Specific Area comparison error

The data in the SSIF and M2TS Specific Areas does not match.

Background

Each SSIF file is associated with two M2TS files. One of these M2TS files includes the normal A/V data for 2D playback (2D Clip). From this file, most of the A/V data is used for the left eye view for 3D playback. The part of the 2D Clip that is not included in the left eye Clip is called the 'M2TS Specific Area'. This data is duplicated and recorded in the SSIF file in the area called 'SSIF Specific Area' **(i.e. data in M2TS Specific Area = data in SSIF Specific Area).** The other M2TS file includes the A/V data for the right eye view for 3D playback. The SSIF file consists of all the A/V data from the left and right eye files.

The following picture shows an example of the file extents in a 3D image.


Extent Block #0
Extent Block #1
Left Eye (2D) Clip
EXT-L
EXT-L
EXT-L
Right Eye Clip
EXT-R
EXT-R
SSIF Clip
SSIF Specific Area
SSIF Specific Area
MT2S Specific Area
Logical Address on disc
Non-AV Data
Identical
Identical

Severity

It is unknown how this may affect playability. Therefore, it is treated as an ERROR.

Cause

This condition is caused by the authoring system that created the image.

Solution

The image must be re-authored. Contact Eclipse Customer Support.

Type:	3D-BD
Reference:	3D Specifications
Default Program Action:	Error

Rule ID: 1742

SSIF file overlaps with a single M2TS file

An SSIF file must overlap with two M2TS files as required by the specifications.

Background

In 3D, each SSIF file is associated with two M2TS files: one for the left eye and one for the right eye. The SSIF file consists (overlaps) of extents from each of the two M2TS files (SSIF = L + R). The SSIF file is created in such a way that it includes data from both left and right eye M2TS files. Therefore, the SSIF file must include extents from at two different M2TS files.

Severity

It is unknown how this condition might affect playability. Therefore, it is treated as an ERROR.

Cause

This condition is caused by the authoring system that created the image.

Solution

The image must be authored. However, as of this writing, the 3D specifications were not yet finalized. Check with the author of the image to verify the severity of this condition.

Type:	3D-BD
Reference:	3D Specifications
Default Program Action:	Error

Rule ID: 1733

SSIF file overlaps with more than two M2TS files

An SSIF file cannot overlap with more than two M2TS files.

Background

In 3D, each SSIF file is associated with two M2TS files: one for the left eye and one for the right eye. The SSIF file consists of extents from each of the two M2TS files (SSIF = L + R). The SSIF file cannot include extents from any more files.

Additional Info

When this condition occurs, the **Additional Info** column in the Analysis will identify the files in question.

'[*SSIF_File*]' overlaps with '[*M2TS_File*]', '[*M2TS_File*]' and '[*M2TS_File*]'

This message identifies the SSIF file and the three M2TS files that are included in the SSIF file.

Severity

It is unknown how this will affect playability. Therefore, this condition is treated as an ERROR.

Cause

This condition is caused by the authoring system that created the image.

Solution

The image must be re-authored. However, as of this writing, the 3D specifications were not yet finalized. Check with the author of the image to verify the severity of this condition.

Type:	3D-BD
Reference:	3D Specifications
Default Program Action:	Error

Rule ID: 1731

SSIF file with no overlapping M2TS files

An SSIF file does not overlap with any M2TS file as required by the specifications.

Background

In 3D, each SSIF file is associated with two M2TS files: one for the left eye and one for the right eye. The SSIF file consists (overlaps) of extents from each of the two M2TS files (SSIF = L + R). The SSIF file is created in such a way that it includes data from both left and right eye M2TS files. Therefore, the SSIF file must include extents from at two different M2TS files.

Severity

It is unknown how this condition might affect playability. Therefore, it is treated as an ERROR.

Cause

This condition is caused by the authoring system that created the image.

Solution

The image must be authored. However, as of this writing, the 3D specifications were not yet finalized. Check with the author of the image to verify the severity of this condition.

Type:	3D-BD
Reference:	3D Specifications
Default Program Action:	Error

Rule ID: 1732

SSIF Specific Area not aligned with AU

The start address of the SSIF Specific Area does not start with an Aligned Unit.

Background

The 3D Specifications require that all extent addresses start at an address that is the beginning of an Aligned Unit.

Severity

It may not be possible to process the image since encryption is performed at the Aligned Unit level. It is unknown how playback systems or other image processing tools may be affected by this condition. Therefore, this condition is considered an ERROR.

Cause

This condition is caused by the authoring system that created the image.

Solution

The image must be re-authored. Contact Eclipse Support for further assistance.

Type:	3D-BD
Reference:	3D Specifications
Default Program Action:	Error

Rule ID: 1741

Stereoscopic content assigned to multiple CPS Units

More than one CPS Unit has references to the Stereoscopic Interleaved file.

Background

The Stereoscopic Interleaved file (SSIF) in a 3D Blu-ray image is described by a since CPS Unit Usage File. Each CPS Unit Usage File also identifies a unique CPS Unit. This condition indicates that more than one CPS Unit Usage Files contain references to the same Stereoscopic Interleaved File (*.SSIF).

Severity

It is unknown if this condition will have any playability problems. However, it is a violation of the specifications and, therefore, considered an ERROR.

Cause

This condition is caused by the authoring application that created the image.

Solution

The image must be re-authored. Contact Eclipse Support for further assistance.

Type:	3D
Reference:	Blu-ray Specifications Annex P: Main requirements for Stereoscopic 3D
Default Program Action:	Error

Rule ID: 1779

Stereoscopic Interleaved file allocation error

The Stereoscopic Interleaved file (SSIF) contains an extent that does not exist on either the left eye (2D) file or right eye file.

Background

The SSIF file consists of extents from both left and right eye files. This condition indicates that the SSIF file includes an extent that is not found on either the left or right eye files.

Severity

It is unknown how this will affect playability. Therefore, it is considered an ERROR.

Cause

This problem is caused by the authoring system that created the image.

Solution

The image must be re-authored. Contact Eclipse Support for further assistance.

Type:	3D
Reference:	Blu-ray Specifications Annex P: Main requirements for Stereoscopic 3D
Default Program Action:	Error

Rule ID: 1765

TBS certificate analysis error

This is a general error that occurs while analyzing a certificate. For the specific cause of this error, please refer to the **Additional Info** column of the Analysis. The possible causes of this error are listed and described in the **Additional Info** section.

Background

As part of the Java security, the EclipseSuite tools will analyze certificates on images that include BD-Java content. Authors use certificates for authentication of the content. In Blu-ray, BD-Java applications and related files are stored in JAR files on the media. To ensure that the applications and related files have not been tampered with, the BD-Java applications and related files are 'signed' during authoring. During the signing process, the signatures are stored in the Signature File. The Signature File is encrypted using the author's private encryption key and it is stored inside the Signature Block File. The author's public key is included inside a certificate within the Signature Block File. The public key is used by applications (e.g. EclipseSuite) and BD-players to validate that the content is still intact.

Additional Info

Since this error can be triggered while analyzing any of the certificate structure fields, the **Additional Info** column of the Analysis will display a message that is specific to the certificate analysis operation that where the error occurred.

Error Conditions When Processing the Root Certificate File

There are two types of root certificates: application root certificate and binding unit root certificate. Both certificates have the same structure as all other certificates. However, the root certificates are each stored in a file of their own: **app_discroot.crt** and **bu_discroot.crt**.

The root certificates are at the top of the certificate chain and they are considered to be a trusted certificate, which means that they do not need to be validated. However, the root certificates are loaded into memory and go through some processing before being analyzed. The following error conditions occur when processing the root certificate.

Reference:

– ***CertFilename*** specifies the root certificate filename. This may be app_discroot.crt or bu_discroot.crt.

– ***SerialNo*** specifies the serial number of the tbsCertificate inside the root certificate.

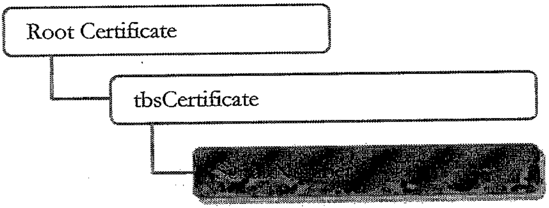
– ***ErrID*** specifies the internal error number.

'[*CertFilename*]': PGPASNUC failed, cert(*0* | *-1*). Error([*ErrID*])

This condition indicates the function that decodes the root certificate failed.

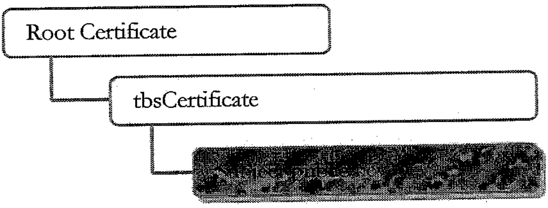
'[*CertFilename*]': GIV failed, cert([*SerialNo*] | [*-1*]). Error(*ErrID*)

This condition indicates that the function that reads the root certificate's serial number failed. The serial number is assigned by the organization that issued the certificate. The issuer and the serial number fields uniquely identify a certificate.



'[*CertFilename*]': PGPASNURSAK failed, cert([*SerialNo*] | *-1*). Error([*ErrID*])

This condition indicates a failure while decoding the public key from the root certificate. The key refers to the issuer's public key that is placed in the root certificate when the image is authored. It is used to validate other certificates.



'[*CertFilename*]': PGPND failed, cert([*SerialNo*] | -1). Error([*ErrID*])

This condition occurs when trying to allocate memory for the tbsCertificate. The function that allocates memory failed. It is possible that are no more memory resources available on the system.

'[*CertFilename*]': PGPASNPTBSC failed, cert([*SerialNo*] | [-*1*]). Error([*ErrID*])

This condition occurs when attempting to encode the tbsCertificate.

The function that analyzes the tbsCertificate requires that the tbsCertificate be encoded. The tbsCertificate was decoded when its parent Certificate was first loaded into memory. Therefore, the EclipseSuite tools will encode the tbsCertificate before passing it to the function that analyzes it. It is during the encoding process that this error occurs.

'[*CertFilename*]': VX509C failed, cert([*SerialNo*] | *-1*). Error([*ErrID*])

This error occurs when trying to analyze the contents of the root Certificate.

The root certificate is passed on to a function that analyzes its contents. This error indicates that at least one of the analysis functions failed. It is likely that you will see other error messages in the next section.

Error Conditions When Analyzing a Certificate

The following error conditions apply to all certificates. The specifications require some minimal check on each certificate. These errors are triggered if one of those checks fails. As shown in Figure 1, the tbsCertificate is recorded inside a Certificate. During this portion of the analysis, it is the tbsCertificate that is being analyzed.

Reference:

- ***JARFilename*** specifies the JAR file in which the Signature Block File that contains the certificate is recorded. The JAR filename format is nnnnn.jar, where n is any digit. In the case of the root certificate, this will specify "disc root".
- ***SignatureBlockFile*** specifies the Signature Block File (SIG-BDxx.RSA) which contains the Certificate in which the tbsCertificate is recorded. In the case when this error occurs on the root certificate, this will specify be the root certificate filename (app_discroot.crt or bu_discroot.crt).
- ***IsIssuer*** is a number that indicates whether the error condition refers to the Issuer or the Subject field in the tbsCertificate. If it is non-zero, then it refers to the Issuer field. Otherwise it is referring to the Subject.
- ***SerialNo*** specifies the serial number of the tbsCertificate being analyzed.
- ***CertIdx*** specifies the index of a Certificate within a certificate chain.
- ***ExtIdx*** specifies the tbsCertificate extension.
- ***NameIdx*** specifies the index of an issuer's name in a sequence of names.

'[*JARFile*]', '[*SignatureBlockFile*]': DNL failed, issuer([*IsIssuer*]), cert([*SerialNo*] | [*CertIdx*])

This condition indicates that an error occurred when trying to determine the length of the Issuer or Subject fields in the tbsCertificate.

'[*JARFile*]', '[*SignatureBlockFile*]': Can't determine issuer([*IsIssuer*]) name, cert([*SerialNo*] | [*CertIdx*])

This condition indicates that the length of the Issuer or Subject fields is invalid.

'[*JARFile*]', '[*SignatureBlockFile*]': PGPND failed, issuer([*IsIssuer*]), cert([*SerialNo*] | [*CertIdx*])

This condition indicates that the EclipseSuite tools were unable to allocate memory in order to read the Issuer or Subject names.

'[*JARFile*]', '[SignatureBlockFile]': DNL failed, issuer([IsIssuer]), cert([*SerialNo*] | [*CertIdx*])

This condition indicates that the EclipseSuite tools were unable to read the Issuer or Subject names.

[*JARFile*]', '[SignatureBlockFile]': Can't determine issuer name, cert([*SerialNo*] | [*CertIdx*])

This condition indicates that the Issuer name is empty.

[*JARFile*]', '[*SignatureBlockFile*]': Can't determine subject name, cert([*SerialNo*] | [*CertIdx*])

This condition indicates that the Subject name is empty.

'[*JARFile*]', '[*SignatureBlockFile*]': URSAK failed, cert([*SerialNo*] | [*CertIdx*])

This condition indicates that an error occurred when decoding the Subject Public Key in the tbsCertificate.

Error Conditions When Analyzing the tbsCertificate Extensions

Certificate extensions are attributes that can be specified for a tbsCertificate. The specifications require that certain extensions be included in a tbsCertificate. The following errors can occur while analyzing the certificate extensions.

Key Usage Extension

The key usage extension defines a structure that contains bit flags which are used to specify usage restrictions of the key contained in the certificate. The structure is as follows:

```
KeyUsage ::= BIT STRING {
        digitalSignature          (0),
        nonRepudiation            (1),
        keyEncipherment           (2),
        dataEncipherment          (3),
        keyAgreement              (4),
        keyCertSign               (5),
        cRLSign                   (6),
        encipherOnly              (7),
        decipherOnly              (8) }
```

The following errors may occur when analyzing this structure.

'[*JARFile*]', '[*SignatureBlockFile*]': DKU failed, KeyUsage, cert([*SerialNo*] | [*CertIdx*] | [*ExtIdx*])

This error condition occurs when trying to decode the Key Usage extension data structure.

'[*JARFile*]', '[*SignatureBlockFile*]': GIV failed, KeyUsage, cert([*SerialNo*] | [*CertIdx*] | [*ExtIdx*])

This error condition occurs when attempting to convert the Key Usage extension data to an integer value.

Issuer & Subject Alternative Names Extension

The issuer and subject alternative names extension allows additional identities to be bound to the issuer and subject of the tbsCertificate. These identities include an email address, a DNS name, an IP address, an URI, and others. The alternative name is specified via the GeneralName structure:

```
GeneralName ::= CHOICE {
        otherName                 [0] OtherName,
        rfc822Name                [1] IA5String,
        dNSName                   [2] IA5String,
        x400Address               [3] ORAddress,
        directoryName             [4] Name,
        ediPartyName              [5] EDIPartyName,
        uniformResourceIdentifier [6] IA5String,
        iPAddress                 [7] OCTET STRING,
        registeredID                 [8] OBJECT IDENTIFIER }
```

The following errors may occur when analyzing the Issuer or Subject Alternative Names extension.

'[*JARFile*]', '[*SignatureBlockFile*]': PKIUPGNs failed, AltSubject, cert([*SerialNo*] | [*CertIdx*] | [*ExtIdx*])
This error occurs when trying to decode the ***Subject Alternative Names*** *extension data.*

'[*JARFile*]', '[*SignatureBlockFile*]': PKIUPGNs failed, AltIssuer, cert([*SerialNo*] | [*CertIdx*] | [*ExtIdx*])
This error occurs when trying to decode the ***Issuer Alternative Names*** *extension data.*

Subject & Authority Key Identifier Extension

The **authority key identifier** extension provides the means of identifying the public key corresponding to the private key used to sign a certificate. This extension is used where an issuer has multiple signing keys.

The **subject key identifier** extension provides a means of identifying certificates that contain a particular public key. It is the same value as the Key Identifier value in the Authority Key Identifier structure.

The structure of the Authority Key Identifier is as follows:

```
AuthorityKeyIdentifier ::= SEQUENCE {
        keyIdentifier              [0] KeyIdentifier OPTIONAL,
        authorityCertIssuer        [1] GeneralNames OPTIONAL,
        authorityCertSerialNumber [2] CertificateSerialNumber OPTIONAL }
```

- **Key Identifier** represents a SHA-1 hash for the public key that is stored in the subjectPublicKey field inside the SubjectPublicKeyInfo structure of the tbsCertificate being analyzed.
- **Authority Certificate Issuer** specifies the Issuer name(s) of the tbsCertificate being analyzed. This field can be one or more GeneralName structures.
- **Authority Certificate Serial Number** specifies the Serial Number of the tbsCertificate being analyzed.

The following error conditions may occur while trying to analyze the Authority Key Identifier extension.

'[*JARFile*]', '[*SignatureBlockFile*]': PKIUOS failed, subjectKeyIdentifier, cert([*SerialNo*] | [*CertIdx*] | [*ExtIdx*])

This error occurs when trying to decode the ***Subject Key Identifier*** *extension data.*

'[*JARFile*]', '[*SignatureBlockFile*]': PGPND failed, subjectKeyIdentifier, cert([*SerialNo*] | [*CertIdx*] | [*ExtIdx*])

This error occurs when trying to allocate memory for the ***Subject Key Identifier*** *extension data.*

'[*JARFile*]', '[*SignatureBlockFile*]': PKIUAKI failed, authorityKeyIdentifier, cert([*SerialNo*] | [*CertIdx*] | [*ExtIdx*])

This error occurs when trying to decode the ***Authority Key Identifier*** *data structure.*

'[*JARFile*]', '[*SignatureBlockFile*]': PGPND failed, authorityKeyIdentifier, cert([*SerialNo*] | [*CertIdx*] | [*ExtIdx*])

This error occurs when trying to allocate memory for the ***key identifier****.*

'[*JARFile*]', '[*SignatureBlockFile*]': **PGPND failed, authorityCertIssuer, cert([*SerialNo*] | [*CertIdx*] | *ExtIdx*)**

This error occurs when trying to allocate memory for the ***authority certificate issuer.***

'[*JARFile*]', '[*SignatureBlockFile*]': **PKIPGN failed, authorityCertIssuer, cert([*SerialNo*] | [*CertIdx*] | [*ExtIdx*])**

This error occurs when trying to load the ***authority certificate issuer*** *into memory.*

'[*JARFile*]', '[*SignatureBlockFile*]': **PKIUGN failed, authorityCertIssuer, cert([*SerialNo*] | [*CertIdx*] | [*ExtIdx*])**

This error occurs when trying to decode the ***authority certificate issuer.***

Since the **Authority Certificate Issuer** may include one or more GeneralName structures, the EclipseSuite tools will process each and trigger any of the following three messages if an error occurs.

'[*JARFile*]', '[*SignatureBlockFile*]': **DNL2 failed, authorityCertIssuer, cert([*SerialNo*] | [*CertIdx*] | [*ExtIdx*] | [*NameIdx*])**

This error occurs when trying to determine the size of the ***authority certificate issuer*** *field.*

'[*JARFile*]', '[*SignatureBlockFile*]': **PGPND failed, authorityCertIssuer, cert([*SerialNo*] | [*CertIdx*] | [*ExtIdx*] | [*NameIdx*])**

This error occurs when trying to allocate memory for the ***authority certificate issuer*** *data.*

'[*JARFile*]', '[*SignatureBlockFile*]': **DNL2 failed, authorityCertIssuer, cert([*SerialNo*] | [*CertIdx*] | [*ExtIdx*] | [*NameIdx*])**

This error occurs when decoding a name from the ***authority certificate issuer.***

'[*JARFile*]', '[*SignatureBlockFile*]': **PKIGIV failed, authorityCertSerialNumber, cert([*SerialNo*] | [*CertIdx*] | [*ExtIdx*])**

This error occurs when attempting to read the ***authority certificate serial number.***

Severity

When any of the certificate analysis checks fail, it is assumed that the certificate authentication failed. If the certificate authentication fails, then it cannot be trusted. Therefore, this rule is considered and ERROR.

Cause

Although certificates are included to validate that the data content has not been altered, the cause for any certificate analysis failure will typically be due to data corruption or data that has not been created properly during authoring.

Solution

Most of the certificate analysis checks above are low-level functions which do not always provide a lot of detail as to the cause of the failure. However, the information above should be enough to give an author clues as to where the failure occurred and how to correct it.

Advanced

All the low-level functions that are used in the certificate analysis return an internal error number (***ErrID***) which may provide additional clues as to the failure. Some of the error conditions above display this number but most do not. The debug information of the analysis will display the error condition (displayed in the Additional Info column) and the internal error number and matching error description.

Type:	Blu-ray
Reference:	Blu-ray Specifications, Section 3-2: BD-Java Specifications
Default Program Action:	Error

Rule ID: 1628

Title assigned to a CPS Unit

An orphaned Title has been assigned to a CPS Unit.

Background

During analysis of a Blu-ray disc, the EclipseSuite tools validate CPS Unit to Clip AV Stream mappings. Clip AV Streams are referenced by Titles. Titles belong to a CPS Unit. All Titles belonging to the same CPS Unit must be encrypted with the same CPS Unit Key. If the EclipseSuite tools find a Title that is not assigned to a CPS Unit (orphaned), the tools check to see if the Clip AV Stream referenced by this Title are referenced by another Title assigned to a valid CPS Unit. If so, then it is assumed that the orphaned Title belongs to the same CPS Unit. The EclipseSuite tools assign the Title to the same CPS Unit and trigger this rule.

Severity

This rule is considered a WARNING since it is letting the user know that a modification is being made to a Title in order to correct a problem.

Cause

This problem is caused by the authoring system that created the image.

Solution

When the image is processed with the EclipseSuite tools, this problem will be corrected.

Type:	Blu-ray
Reference:	AACS Blu-ray Pre-recorded Book Revision 0.92
Default Program Action:	Warning

Rule ID: 841

Title Key File is on layer 1

The file Unit_Key_RO.inf or its duplicate is located on Layer 1.

Background

The BDCMF specification states that all CPS Unit Key Files, also known as Title Key Files, should be ocated on Layer 0, even for Dual Layer titles.

The CPS Unit Key File is stored on the disc as the file Unit_Key_RO.inf. This file must reside in the AACS directory and a copy of the file must be located in the AACS\DUPLICATE directory. It is recommended practice that the authoring system place both of these files on layer 0.

In the Blu-ray encryption system, the title key files are encrypted using the Volume ID. The Volume ID is generated at mastering of the layer and is linked to a particular LBR's ROM Mark Inserter. This means that the encryption of the title keys on layer 0 and layer 1 will not match if a different LBR is used to master each layer. This is a problem because Blu-ray drives typically only use the layer 0 volume ID for decryption purposes.

As a result, when title keys are placed on layer 1 it creates a situation where layer 0 and layer 1 must be mastered on the same LBR in order to ensure the proper encryption and decryption of the title key files. Otherwise it is possible that the title keys on layer 1 will not be accessible using the layer 0 Volume ID.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will identify the title key file by name.

Unit_Key_RO.inf: The primary title key file is on layer 1.
Duplicate Unit_Key_RO.inf: The duplicate title key file is on layer 1.

Severity

This rule is treated as an error. Even though the specification only recommends placing all title key files on layer 0, there are serious process concerns if a title key file is placed on layer 1 and attention should be drawn to the rule.

Possible Cause

The authoring system that created the image did not follow the recommended guideline of putting all Title Key Files on layer 0.

Possible Solution

The image should be re-authored to correct this condition.

When using Eclipse ImageEncoder, this condition can be tolerated if the process can be controlled properly. If the same LBR is used to master both layers, there should be no difference in the Volume ID or Title Key Files and no potential for decryption errors.

Type:	Blu-ray
Reference:	BDCMF 1.01 Appendix B Section 5.3
Default Program Action:	Error

Rule ID: 1565

Title Key File replaced

This is an informational message that indicates that the Unit_Key_RO.inf file was successfully replaced during the mastering process.

Background

The CPS Unit Key file (Unit_Key_RO.inf) contains the encryption keys (Title Keys) that are used to encrypt the ClipAV files. The Blu-ray specifications require that this file be encrypted on a Blu-ray disc. Therefore, during mastering of a Type C image, one of the last steps that Eclipse's ImageEncoder must do is to encrypt this file. This is done in memory as the encoder is processing the data. The original Type C image remains unchanged.

Type:	Exclude
Reference:	AACS Specifications
Default Program Action:	Info

Rule ID: 883

Title Key File replacement failure

An error occurred when replacing the Unit_Key_RO.inf file.

Background

During normal processing of a Blu-ray image, there are some files that are replaced. One of them is the Unit_Key_RO.inf file. This file is encrypted and replaced by the encoder system during mastering. It is during this process that this error might occur.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display more details.

Encrypted file data '[*Filename*]' too short

The file data is loaded into memory then it is encrypted. The encrypted data is shorter than the file size on the image.

Image file data '[*Filename*]' too short

The file is loaded into memory then it is encrypted. The encrypted data is longer than the file on the image.

Severity

This condition indicates a serious problem and it is therefore considered an ERROR.

Cause

It is unknown what causes this condition.

Solution

Contact Eclipse Customer Support.

Type:	MainChannel
Reference:	AACS Specifications
Default Program Action:	Error

Rule ID: 882

Title missing from Unit Key RO file

The file Unit_Key_RO.inf is missing a reference to a Title.

Background

The index.bdmv and the Unit_Key_RO.inf files contain references to Titles. Both files must have the same references to the same Titles. This rule is triggered when a title is found in the index.bdmv but not in the Unit_Key_RO.inf file. This is a critical error since the Unit_Key_RO.inf file contains a relationship between Titles and the CPS Unit Key that will be used to encrypt them. If the Title reference is not present on this file, then it will be impossible for a player to know which CPS Unit Key to use to decrypt the Title during playback.

During the ImageCopy encryption process, ImageCopy always follows the AACS1.DAT file. This file specifies the clip files and the CPS Unit Key that will be used to encrypt it. Therefore, there is no need to parse the Unit_key_RO.inf and Titles to find the commands that reference the clip files.

Severity

This rule is considered an ERROR since it is known to cause playability problems.

Cause

This condition is caused by the authoring system since it is responsible for creating the Unit_Key_RO.inf file.

Solution

This problem cannot be corrected in pre-mastering or mastering. The image must be re-authored.

Type:	Blu-Ray
Reference:	N/A
Default Program Action:	Error

Rule ID: 1506

Title not included in CPS Unit Usage File

A Title is specified in the CPS Unit Key file but not in the CPS Unit Usage file.

Background

The CPS Unit Key file (Unit_Key_RO.inf) includes a list of all Titles on a Blu-ray Video image. Each Title is assigned to a CPS Unit. For every CPS Unit there is an associated CPS Unit Usage file (CPSUnitXXXXX.cci), which includes a list of the Titles in the CPS Unit. This rule indicates that the CPS Unit Key file included a Title but the same Title was not listed in the corresponding CPS Unit Usage file.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will identify the Title.

Severity

This condition is considered an ERROR since it may cause playability problems.

Cause

This condition is caused by the authoring application that created the image.

Solution

The image must be re-authored. Consult with the customer or company who authored the image. Contact Eclipse Customer Support for further assistance.

Type:	Blu-Ray
Reference:	N/A
Default Program Action:	Error

Rule ID: 1874

Title Structure file error

The Title Structure file is missing an attribute or the attribute has an unknown value.

Background

A Title Structure file is an external file that defines the authoring layout of a Blu-ray image. Eclipse has created the title structure file so that a movie studio can create a custom layout that meets their authoring requirements for Blu-ray. Once this title structure is defined, the Eclipse software checks the image to make sure it complies with the title structure requirements.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display more details about the condition that triggered this rule.

Severity

This error indicates that the image being analyzed did not conform to the title structure requirements. Therefore, this condition is considered an ERROR.

Cause

This condition is normally caused during authoring of the image.

Solution

This error does not indicate any problem with the Blu-ray format. It is an error that gets triggered when the layout of the image does not conform to a predefined layout specified by the movie studio. Check with the authoring or movie studio whether it is ok to continue with the image or whether the image should be re-authored.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

Rule ID: 1609

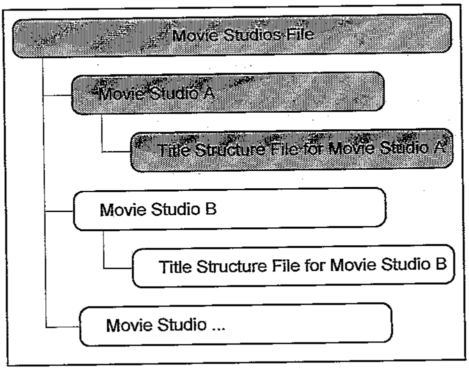
Title Structure not checked

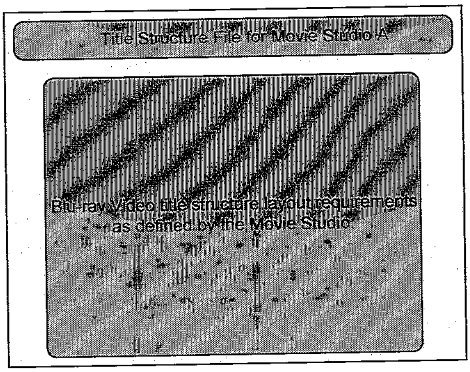
Title Structure Analysis is not performed because of a failure or because the image movie studio does not match any of the internal movie studio configuration files.

Background

The EclipseSuite applications include embedded movie studio and title structure configuration files. The Movie Studios file identifies all the 'known' movie studios. It identifies one or more producers (authors) for the movie studio. Each movie studio entry has a link to a Title Structure file. It also provides other basic movie studio configuration.

In the Title Structure file, each movie studio can define the layout of a Blu-ray Video. The purpose of this is to always have a consistent title structure layout.


Movie Studios File
Movie Studio A
Title Structure File for Movie Studio A
Movie Studio B
Title Structure File for Movie Studio B
Movie Studio ...


Title Structure File for Movie Studio A
Blu-ray Video title structure layout requirements as defined by the Movie Studio

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display more details with one or more of the following messages.

The following conditions may occur when parsing the Movie Studios configuration file.

Failed to load '[*Filename*]'

This message indicates that the Eclipse software failed to load the file that contains the Movie Studio information. This file includes a list of Movie Studios and a link to the Title Structure file that is to be used when analyzing an image produced by the movie studio. If the movie studio cannot be identified, then the Title Structure analysis cannot be performed.

This can also occur when trying to read the version of the Movie Studio file and no version information is found. If this occurs when using an external movie studio file, the Eclipse software attempts to load an internal copy of the same file. This error indicates that an error occurred when loading the internal copy from its resources.

This can also occur when the version is older than expected. If using an external file, the Eclipse software will try loading the internal copy. This condition occurs it is unable to load the internal file.

'[*Filename*]'. [*ErrorDesc*]. Line: [*LineNo*], Col: [*ColNo*]

This message indicates that the Eclipse software was able to load the file that contains the Movie Studio information. Unfortunately, an error occurred when parsing the file. This file includes a list of Movie Studios and a link to the Title Structure file that is to be used when analyzing an image produced by the movie studio. If the movie studio cannot be identified, then the Title Structure analysis cannot be performed.

This can also occur when trying to read the version of the Movie Studio file and no version information is found. If this occurs when using an external movie studio file, the Eclipse software attempts to load an internal copy of the same file. This error indicates that it successfully load the internal movie studio file but a parsing error occurred.

This error also occurs when the version is older than expected. Originally we were using external file but switch to internal file. Loaded internal file ok but a parsing error occurred.

This message shows the internal error description along with a line and column numbers in the Movie Studio file where the parsing error occurred.

'[*Filename*]', '\MovieStudioList\Version' text element not found

This message indicates that the Eclipse software was able to load the file that contains the Movie Studio information. Unfortunately, the version attribute/value is not present.

'[*Filename*]' version is [*Actual*] instead of [*Expected*]

This message indicates that the Movie Studio file version is older than expected.

'[*Filename*]'. Unknown 'MovieStudio'

This message indicates that a Movie Studio entry in the MovieStudio.xml file does not specify an Application Root Certificate. Therefore, the Eclipse software cannot determine the owner of the image and cannot continue with the Title Structure analysis.

'[*Filename*]'. Unknown 'MovieStudio' with app root cert '[*AppRootCert*]'

This message indicates that a Movie Studio entry in the MovieStudio.xml file includes an application root certificate but it does not match any of the application root certificates in the image. Therefore, the Eclipse software cannot determine the owner of the image and cannot continue with the Title Structure analysis.

'[*Filename*]'. 'TitleStructureFile' for 'MovieStudio' '[*MovieStudioName*]' not found

This message indicates that a Movie Studio entry in the MovieStudio.xml file does not specify a Title Structure file.

The following conditions may occur when parsing the Title Structure file.

Failed to load '[*TitleStructureFile*]'

This message indicates that the Eclipse software was unable to load the external or internal Title Structure files. Therefore, the Eclipse software cannot continue with the Title Structure analysis.

'[*TitleStructureFile*]'. [*ErrorDesc*]. Line: [*LineNo*], Col: [*ColNo*]

This message indicates that an error occurred when parsing the Title Structure file, indicating that the file may be corrupt.

'[*TitleStructureFile*]', '\TitleStructure\Version' text element not found

This message indicates that the version element in the Title Structure file is missing.

'[*TitleStructureFile*]' version is [Actual] instead of [*Expected*]

This message indicates that the version of the Title Structure file is older than expected.

'[*TitleStructureFile*]'. '\TitleStructure\MovieStudio', 'Name' attribute '[*MovieStudio*]' not found

This message indicates that the Eclipse software was unable to read the Movie Studio name from the Title Structure file.

'[*TitleStructureFile*]'. Couldn't find a 'Layout' that applies to '[*Timestamp*]'

This message indicates that the Eclipse software was unable to find a Title Structure layout that matches the current image (the recording date/time of the image is blank).

'[*TitleStructureFile*]'. Couldn't find 'Layout' with 'TimeStamp' attribute '[*Timestamp*]'

This message indicates that none of the Title Structure layouts in the Title Structure file match the current image. The layout timestamp must match with an image's recording data/time.

A critical error occurred

This message indicates that an unexpected error occurred while performing the Title Structure analysis. The Title Structure analysis is aborted.

Severity

This rule does not indicate a problem with the Blu-ray Video. Therefore, it is only considered a FLAG severity.

This rule is triggered when an unknown Movie Studio is found. However, it may also indicate a problem in the processing of the Title Structure and/or Movie Studio file(s). This will be indicated with one or more of the conditions listed above.

Cause

As Movie Studio and Title Structure configuration files are updated with new or modified requirements, it is possible that older images may no longer conform to the new changes. Therefore, one common cause is analyzing an older image that no longer conforms to the current Movie Studio Title Structure layout requirements.

If it is a new image, it is also possible that authoring studios may not be conforming to the same Movie Studio Title Structure layout as the EclipseSuite applications, or vice versa.

Solution

This error does not indicate any problem with the Blu-ray format. It is an error that gets triggered when the layout of the image does not conform to a predefined layout specified by the movie studio. Check with the authoring or movie studio whether it is ok to continue with the image or whether the image should be re-authored.

Also, make sure that you are running the most current EclipseSuite version to ensure that you are using the most current Title Structure configuration files.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Flag

Rule ID: 1665

Transport stream recording rate exceeded

The recording rate of a Clip AV file exceeds the maximum allowed by the specifications.

Background

A Clip's recording rate is stored in the Clip Information File (#####.clpi). During the analysis of the image, the EclipseSuite tools recalculate the recording rate of each Clip and compare it to the value stored in the Clip Information file. If the recalculated value is higher than the value specified in the Clip Information file, then this rule is triggered.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will show the actual and expected values.

'#####.m2ts': actual (*ActualRecordingRate*) bytes/second, expected (*ExpectedRecordingRate*) bytes/second

This message identifies the Clip file whose recording rate does not match the recalculated recording rate.

Severity

It is unknown if this condition will cause playability problems. However, it is a violation of the Blu-ray specifications and it is, therefore, considered an ERROR.

Cause

This condition is caused by the authoring application that created the image.

Solution

The image must be re-authored.

Type:	Blu-ray
Reference:	Blu-ray Audio/Video Specifications
Default Program Action:	Error

Rule ID: 1550

Triple layer (Opposite Track Path)

This is an informational rule that identifies a Blu-ray Triple Layer Opposite Track Path image.

Type:	Exclude
Reference:	None
Default Program Action:	Info

Rule ID: 1902

Unable to retrieve CHT from image

This rule is triggered when a Content Hash Table (CHT) cannot be loaded from an AACS encrypted image. It applies to Type B, Type C, & Type D images and replicas.

Background

When analyzing or verifying an AACS encrypted image, the EclipseSuite BD analysis engine calculates a CHT for an image and compares it to the actual CHT found in the image.

For each physical layer of BD-ROM, the Content Hash Table (CHT) is stored in the "\AACS" directory and in the "\AACS\DUPLICATE" directory. A single-layer disc has a single file named "ContentHash000.tbl"; a dual-layer disc has two files named "ContentHash000.tbl" for Layer 0 and "ContentHash001.tbl" for Layer 1. The ContentHash000.tbl and the ContentHash001.tbl are stored on Layer 0 and Layer 1 respectively.

Because this is caused by a corrupt file, this rule will generally be accompanied by other warnings and errors relating to the UDF file system.
Certain additional CHT tests are skipped when then this rule is invoked.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will identify the data it was unable to retrieve with one of the following messages.

L0 - unable to compare

This error occurs when unable to read the file \AACS\ContentHash000.tbl

Duplicate L0 - unable to compare

This error occurs when unable to read the file \AACS\DUPLICATE\ContentHash000.tbl

L1 - unable to compare

This error occurs when unable to load the file \\AACS\\ContentHash001.tbl

Duplicate L1 - unable to compare

This error occurs when unable to load the file AACS\DUPLICATE\ContentHash001.tbl

Error Severity

This rule is considered an error because the Content Hash Tables are required files.

Possible Cause

CHT file is corrupt.

Solution

The image should be recreated from a known good source.

Type:	Blu-ray
Reference:	N/A

Default Program Action: Error

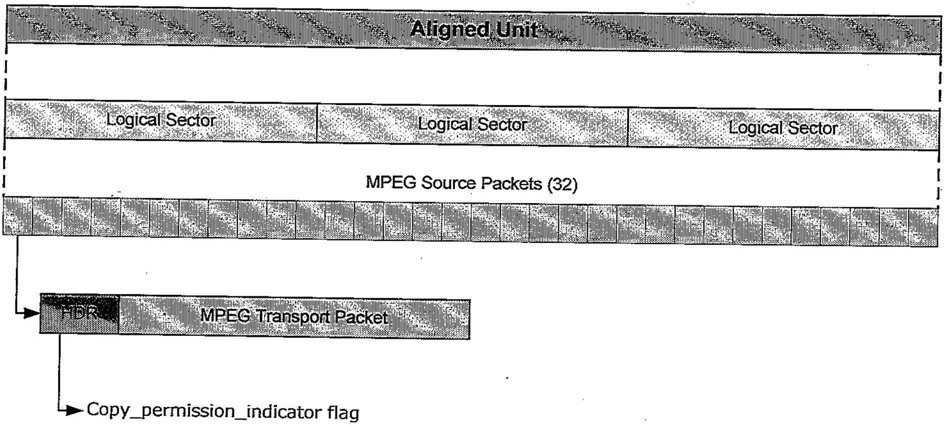
Rule ID: 887

Unencrypted aligned unit has CPI bits set

The protection status of an Aligned Unit indicates that it is (or requires to be) encrypted. However, the Aligned Unit is part of a Clip file that is assigned to an un-encrypted CPS Unit.

Background

Clip files consist of Aligned Units which are 3 logical sectors long. The Copy Protection Indicator bits in the Align Unit indicate the protection status of the Aligned Unit. When a Clip file is assigned to a CPS Unit that is encrypted, then ALL of the Aligned Units in the Clip file must be set to indicate that they are encrypted. Similarly, if a Clip file is assigned to a CPS Unit that is not encrypted, then ALL the Aligned Units in the Clip file must be set to indicate that they are not encrypted.



Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will identify the Clip file that is affected by this error.

'[*Filename*]'

This message identifies the Clip file (#####.m2ts) that contains the Aligned Unit that triggered this error.

Severity

This condition is considered an ERROR since it may lead to playability problems. However, if you are using ImageCopy, this condition will be corrected automatically during the encryption process. Although the error is reported, the resulting output image should no longer have this problem. In that case, this error can be ignored. However, it is highly recommended that the output image is analyzed to ensure that the error no longer exists.

Cause

This problem is caused by the authoring system that created the image.

Solution

This condition will be corrected automatically by ImageCopy during the encryption process. Although the error is reported, the resulting output image should no longer have this problem. In that case, this error can be ignored. However, it is highly recommended that the output image is analyzed to ensure that the error no onger exists.

Type: Blu-ray
Reference: AACS Specifications
Default Program Action: Error

Rule ID: 1571

Unencrypted aligned unit in encrypted CPS Unit

The EclipseSuite applications found an unencrypted Aligned Unit that belongs to a file which is assigned to an encrypted CPS Unit.

Background

A CPS Unit is a group of Titles to which the same Title Key has been assigned. A CPS Unit includes a flag that indicates whether it is encrypted. When a CPS Unit is encrypted, all Clip AV files belonging to the same CPS Unit are also encrypted. Although the Aligned Units in a Clip AV file can be individually tagged for encryption, the specifications require that all Aligned Units in the Clip AV file must be tagged and encrypted if the file belongs to an encrypted CPS Unit. Unfortunately, early on in the life of the Blu-ray format, this requirement was not clear among authoring and encryption applications. Therefore, there may be some early images which did not have all Aligned Units tagged for encryption. During encryption, only the Aligned Units that were tagged were encrypted.

If a Clip AV file contains Aligned Units that are tagged for encryption but the CPS Unit to which the file belongs to is not encrypted, then it could lead to playability problems. Current versions of ImageCopy will automatically correct this condition during the encryption process of the image.

Additional Info

When this rule is triggered, the **Additional Info** column in the analysis will identify the Clip AV Stream file that contains the unencrypted Aligned Unit.

Severity

This condition has the potential of causing playability problems. Therefore, it is considered an ERROR. Typically, when a CPS Unit is encrypted, all Clip files in the same CPS Unit are encrypted. If all Aligned Units in a Clip AV file are not tagged for encryption, it is likely not a problem. However, if the Aligned Units of a Clip file are tagged for encryption and the Clip file belongs to a CPS Unit that is not encrypted, then this condition is likely to cause a problem.

Cause

This condition is created during the authoring process.

Solution

This condition can only be fixed by re-authoring of the image.

Type:	Blu-ray
Reference:	AACS Specifications
Default Program Action:	Error

Rule ID: 1552

Unencrypted CPS Unit contains Enhanced title

An Enhanced Title, which requires to be encrypted, is referenced by an unencrypted CPS Unit.

Background

A CPS Unit refers to a group of Titles to which the same Title Key has been assigned. CPS Units can be encrypted on un-encrypted. Titles are categorized as Basic or Enhanced. Since Enhanced Titles must be encrypted, they cannot be in a CPS Unit that is not encrypted.

Severity

This condition is a violation of the AACS specifications and, therefore, is considered an ERROR.

Cause

This problem is introduced during the authoring of the image.

Solution

This problem can only be corrected by re-authoring the image.

Type:	Blu-ray
Reference:	AACS Specifications
Default Program Action:	Error

Rule ID: 1540

Unencrypted CPS Unit Key

An encrypted image (Type D) or disc contains an unencrypted CPS Unit Key.

Background

The CPS Unit Key refers to the file "Unit_Key_RO.inf". This file stores a unique CPS Unit Key (Title Key) for each CPS Unit that is encrypted with AACS. This file is stored in the \AACS folder and a duplicate copy in the \DUPLICATE folder. One of the steps in the mastering process is to encrypt the CPS Unit Key file prior to encoding. During playback, the Blu-ray players decrypt the file in order to retrieve the CPS Unit Keys that will be used to decrypt the user data.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display the following message.

CPS Unit ([*CPSUnitNo*]), '[#####.m2ts]'

This message identifies the CPS Unit Number (Title Key number) and Clip file that are affected by this error.

Severity

During playback, a BD player assumes that the CPS Unit Key file is encrypted. The process of un-encrypting a CPS Unit Key file that is not encrypted will yield corrupt Title Keys. If the corrupt Title Keys are used to decrypt the user data, then it will lead to playability problems. Therefore, it is considered an ERROR.

Cause

This condition is caused by the utility that created the Type D image. If it occurs on a replicated disc, then it may also be caused by the encoder that mastered it.

Solution

If the problem occurs on a Type D image, it may be possible to correct if the image is converted back to a Type C. It may be possible to do this using Eclipse's CMU utility. However, you should analyze the resulting image to confirm the problem no longer exists.

If the problem occurs on a disc, it may also indicate a problem with then encoder system. Check with the encoder manufacturer for further assistance.

Type:	Blu-ray
Reference:	AACS Specifications
Default Program Action:	Error

Rule ID: 1573

Unexpected Application Root Certificate

The explanation for this title check rule contains confidential information. Please refer to the studio-specific supplemental rules help PDF document. The document is available from Eclipse Support.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

Rule ID: 1653

Unexpected BDCMF file size

******* The description of this rule is not available as it contains confidential information.*******

For more information, please contact Eclipse Customer Support.

Eclipse Customer Support
Phone: (925) 598-0300
Email: Support@eclipsedata.com

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

Rule ID: 1792

Unexpected BDCMF path

The explanation for this title check rule contains confidential information. Please refer to the studio-specific supplemental rules help PDF document. The document is available from Eclipse Support.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

Rule ID: 1743

Unexpected Binding Unit Root Certificate

The explanation for this title check rule contains confidential information. Please refer to the studio-specific supplemental rules help PDF document. The document is available from Eclipse Support.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

Rule ID: 1667

Unexpected Disc Organization ID

The Organization ID specified in the application root certificate does not match any of EclipseSuite's internal list of Organization IDs for known producers.

Background

The Eclipse software maintains a list of Organization IDs for known producers (authoring studios) for a particular movie studio. As part of the Title Structure checks, the Eclipse software identifies the movie studio and producer of Blu-ray Video images. Then it verifies that both match with the same studio and producer in its internal lists. This error indicates that the producer did not match.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will identify the profile with the following messages.

'[*OrganizationID*]'. MovieStudio: '[*MovieStudio*]'. Producer: '[*Producer*]'

This message identifies the movie studio, producer and Organization ID of the producer.

Severity

The Title Structure checks are created by the movie studios so that the authoring studios can create Blu-ray mages in a consistent layout. This error indicates that the image being analyzed did not conform to the title structure requirements. Therefore, this condition is considered an ERROR.

Cause

This condition is normally caused during authoring of the image.

Solution

This error does not indicate any problem with the Blu-ray format. It is an error that gets triggered when the layout of the image does not conform to a predefined layout specified by the movie studio. Check with the authoring or movie studio whether it is ok to continue with the image or whether the image should be re-authored.

Type:	Blu-ray
Reference:	Blu-ray Specifications, Section 3-2: BD-Java Specifications
Default Program Action:	Error

Rule ID: 1664

Unexpected Producer JAR file name

The explanation for this title check rule contains confidential information. Please refer to the studio-specific supplemental rules help PDF document. The document is available from Eclipse Support.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

Rule ID: 1670

Unrecognized HDMV AACS stream

A Clip AV Stream file (*.m2ts) was encrypted with an unknown CPS Unit Key.

Background

The Blu-ray format maintains a relationship between CPS Units, Titles, Movie Objects, Playlists, PlayItems and ClipAV files. A CPS Unit is a group of Titles that are assigned the same Title Key. Titles include references to Movie Objects; Movie Objects include references to Playlists; Playlists include references to PlayItems and PlayItems include references to Clip AV Stream files.

A CPS Unit includes a flag that indicates whether it is encrypted. If it is encrypted, then all Clip AV Stream files that belong to the same CPS Unit must also be encrypted. A Clip AV Stream file is divided into Aligned Units, each consisting of 3 logical sectors.

During the analysis of an encrypted BD image, the EclipseSuite applications determine which Title Key was used to encrypt the files in each CPS Unit. This error indicates that a Clip AV Stream file cannot be decrypted using the Title Key assigned to the CPS Unit that it belongs to. Decryption of the Clip AV file will not be possible.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will identify the Clip AV file.

Severity

This condition is considered an error since a Clip file cannot be decrypted, which will likely cause playability problems.

Cause

This problem is typically caused by the utility that encrypted the image.

Solution

This problem may be corrected by re-encrypting the original image.

Type:	Blu-ray
Reference:	AACS Specifications
Default Program Action:	Error

Rule ID: 1553

Unrecognized HDMV stream

The EclipseSuite tools were unable to recognize the data in the video stream.

Background

Blu-ray Video uses the MPEG format structure. During analysis, the EclipseSuite tools first un-encrypt the data if necessary then analyzes it. This rule indicates that the EclipseSuite tools found data that did not conform to the MPEG structure. However, this is common in images that include 'dummy' content. For example, images that support online transactions where users are able to download a file from an online server. The author might use a dummy file in order to reserve space on the media.

Additional Info

When this rule is triggered, the **Additional Info** column will identify the Clip file that triggered this rule.

'[*Filename*]'

This message identifies the Clip file that triggered this rule. Check with the author of the image to confirm whether this file contains dummy data or if should contain real MPEG data. If it is dummy data, then this rule can be ignored. If it should contain real MPEG data, then this image should be re-authored.

Severity

This rule is considered a WARNING since the EclipseSuite tools are unable to determine if the content is part of a dummy file.

Cause

This may be a condition that is intended by the author.

Solution

Check with the author to confirm that the file identified does contain dummy content. If it is a dummy file, then you can continue processing the image. However, if it supposed to contain valid data, then this image should be re-authored.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Warning

Rule ID: 1566

Unused CPS Unit

The EclipseSuite tools detected an unused CPS Unit number value.

Background

The CPS Unit Key file (Unit_Key_RO.inf) specifies the total number of CPS Units on a disc. It also specifies the CPS Unit number that is assigned to each Title. The CPS Unit numbers increment sequentially starting with the value 1. This rule is typically triggered when the CPS Unit numbers did not increment sequentially.

Additional Info

When this rule is triggered, the Additional Info column in the Analysis will identify the unused CPS Unit numbers.

Severity

Although the specifications state that the CPS Unit numbers should increment sequentially starting at 1, it is unlikely that it will cause any playability problems. Therefore, this condition is considered a WARNING.

Cause

This is caused by the authoring application that created the image.

Solution

The image must be re-authored to correct this condition. However, you should consult with the customer or the company that authored the image.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Warning

Rule ID: 1873

Using newer Title Structure configuration

The disc version in the Disc Properties file is older than the current version.

Background

EclipseSuite 4.0 Beta N (June 2011) implemented a new version of the Title Structure Analysis for Fox & MGM studios. This rule indicates that the image being analyzed meets most of the pre-requisites so that the new Title Structure analysis can be performed. However, the disc version has a value that is older than what was expected. The EclipseSuite tools will apply the new Title Structure Analysis when processing the image.

Severity

This condition is considered an ERROR since the EclipseSuite tools are expecting a newer value for the disc version. This might indicate that the image does not conform to Fox's Title Structure specifications.

Cause

This problem is caused during authoring of the image.

Solution

Consult with Fox Studios to see if this condition is acceptable to continue or whether the image should be re-authored.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

Rule ID: 1859

Using newer Title Structure file

The external MovieStudios.xml or Title Structure file does not have a version specified. Therefore, the EclipseSuite tool will use their internal copy instead.

Background

The Movie Studio (MovieStudios.xml) and Title Structure files are part of the Title Structure analysis. These files specify the Blu-ray disc layout requirements of a movie studio. The files have version numbers which are used to specify the structure of the files. If the version number is not specified, it is assumed that the files are old. The EclipseSuite tools maintain an internal copy of both file. The internal copy is considered current as of when the EclipseSuite tools were created. If the version of the external file is not specified, then the EclipseSuite tools use their internal copy and this rule is triggered to indicate that.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display more details with one of the following messages.

'[*Filename*]', '\MovieStudioList\Version' text element not found

This message indicates that the version number was not specified in the MovieStudios.xml file. The EclipseSuite tools will use their internal copy of the MovieStudios.xml file instead.

'[*Filename*]' version is [Actual] instead of [*Expected*]

This message indicates that the version of the external MovieStudios.xml or Title Structure files is older than expected. The EclipseSuite tools will use the more current version from its internal copy.

[*Filename*]', '\TitleStructure\Version' text element not found

This message indicates that the version number was not specified in the Title Structure file. The EclipseSuite tools will use their internal copy of the Title Structure file instead.

Severity

The Title Structure checks are created by the movie studios so that the authoring studios can author Blu-ray images in a consistent layout. This rule indicates that the Movie Studios or Title Structure file in the application directory may be an old version.

Cause

This condition can occur if the Movie Studio or Title Structure files are not updated along with the EclipseSuite software. It can also occur if the EclipseSuite applications are executed outside their installation directory.

Solution

Verify that the EclipseSuite application is being executed from the installation directory. Also, verify that the Movie Studios (MovieStudios.xml) and Title Structure (*TitleStructure.xml) files are present in the installation directory.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

Rule ID: 1668

Using Older Title Structure configuration

The image is missing the Disc Properties file and, therefore, the EclipseSuite tools cannot apply the most current Title Structure Analysis.

Background

EclipseSuite 4.0 Beta N (June 2011) implemented a new version of the Title Structure Analysis for Fox & MGM studios. This new version requires a Disc Properties file to be present. If this file is not present, then it is assumed that the image does not conform to this new version of the Title Structure. Therefore, the EclipseSuite tools will apply an older version of the Title Structure Analysis.

Severity

This condition is considered an ERROR since it may indicate that this is a new image that was authored not in conformance with Fox's Title Structure.

Cause

This condition is caused during authoring of the image.

Solution

Consult with Fox studios to confirm whether this condition is acceptable to continue or whether the image should be re-authored.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Error

Rule ID: 1858

Using Volume ID found in CMF Data

The Volume ID found in the BDCMF will be used for mastering the image.

Background

The Volume ID is an identifier used in a Blu-ray disc. The Volume ID is typically obtained from Sony's RIT-2000 device and recorded onto the disc during mastering. When a BD image is mastered, the Eclipse ImageEncoder saves the Volume ID in the BDCMF.CMF file so that it is available when mastering layer 1 or if either layer is re-mastered. This rule indicates that this image has already been assigned a Volume ID in the BDCMF.CMF file and has been confirmed to match the Volume ID of the RIT-2000 unit connected with the ImageEncoder system. Therefore, the Volume ID from the BDCMF.CMF will be used to master the image.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display more details with one of the following messages.

Contents verified

The Volume ID from the BDCMF.CMF file match the Volume ID from the RIT-2000 system.

Unable to verify contents

The BDCMF.CMF file includes a Volume ID but the ImageEncoder could not retrieve the Volume ID from the RIT-2000 system to compare to. It is possible that the RIT-2000 system is not responding or it is not connected. ImageEncoder will use the Volume ID from the BDCMF.CMF file.

Severity

This rule does not indicate an error. It is an informational message to let the user know which Volume ID will be used for mastering.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Flag

Rule ID: 1452

Video frame-rate support is optional

The Blu-ray Video image includes MPEG-2, MPEG-4 or VC-1 video at 25Hz and/or 50Hz video frame rate. This combination of video codecs and frame rates may not be supported by all BD-ROM Players unless a 50Hz TV system is used.

Background

Decoding of 25Hz/50Hz video is mandatory only in countries where a 50Hz TV system is used for both HDTV and SDTV (e.g. European countries). In all other countries, it is recommended but not required to support these video frame rates. Therefore, this condition is only a problem if the user attempts to playback on a TV that does not support these video frame rates. For example, a Blu-ray Video with MPEG-2, MPEG-4 or VC-1 video at 25Hz and/or 50Hz video frame rate may fail playback in the United States since players in the United States are not required to support these video frame rates (i.e. the United States uses a 60Hz TV system). The same Blu-ray Video will likely play without problems in European countries since European countries use a 50Hz TV System.

Severity

This condition may be a problem if the Blu-ray Video is played back on a TV system that does not support 25Hz or 50Hz video frame rate. For this reason, this rule is set to a WARNING only.

Cause

It is during authoring where it is determined the type of video a movie will include. It is the author's responsibility that the proper video format is used for the target region (countries). However, this does not prevent consumers to playback in a TV system that it was not intended for.

Solution

This condition does not necessarily indicate a problem. Contact Eclipse Customer Support for further assistance.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Warning

Rule ID: 1783

Volume ID Regenerated

The ImageEncoder has regenerated the Volume ID since the expected value is not available or it is invalid.

Background

The Volume ID is an identifier used in a Blu-ray disc. The Volume ID is typically obtained from Sony's RIT-2000 device and recorded onto the disc during mastering. When a BD image is mastered, the Eclipse ImageEncoder saves the Volume ID in the BDCMF.CMF file so that it is available when mastering layer 1 or if either layer is re-mastered.

This rule is triggered if mastering a BDCMF image that already includes a Volume ID but does not match the Volume ID from the RIT-2000. When this happens, ImageEncoder will use the Volume ID from the RIT-2000 and overwrite the one in the BDCMF. This rule is expected if an image is re-mastered using a different RIT-2000.

Severity

This condition is not considered a problem as long as both layers in a dual-layer BD image is mastered with the same Volume ID.

Cause

This problem occurs when a BDCMF image is already assigned a Volume ID but, when mastered, the Volume ID does not match the one from the RIT-2000.

Solution

Since a different Volume ID will be expected if an image is re-mastered with a different RIT-2000, then there is nothing that needs to be done as this rule would only be indicating a difference in Volume ID, not an error condition.

Type:	Blu-ray
Reference:	N/A
Default Program Action:	Warning

Rule ID: 1454

X.509 certificate issuer

This is an informational message that identifies the entity (e.g. organization) that issued a certificate.

Background

To validate that BD-Java applications and related files have not been compromised, authors provide a digital signature in certificates inside the Signature Block File. The EclipseSuite tools analyze all certificates and their digital signatures to make sure they match the BD-Java content on the image. As each certificate is analyzed, the issuer of that certificate is identified with this rule.

Type:	Blu-ray
Reference:	Blu-ray Specifications, Section 3-2: BD-Java Specifications
Default Program Action:	Info

Rule ID: 1634

Xlet permission not allowed by application profiles

A BD-J application permission that has been specified in the permission request file is not allowed by the application profile.

Background

Permission Request files are used to specify the permissions granted to a BD-J application. However, there are permissions which require a specific application profile. An application profile indicates the BD player profile needed for the application to run.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will identify the profile with the following messages.

'[*BDJOFile*]' [*AppID*], '[*JARFile*]', '[*PermissionRequestFile*]' '[*Permission*]'

This message identifies the permission that triggered this rule.

'[*BDJOFile*]' [*AppID*], '[*JARFile*]', '[*PermissionRequestFile*]' '[*Permission*]' **'value'='true'**

This message identifies the permission that triggered this rule.

Severity

This condition indicates that there is a mismatch in the BD-J application profile and the permission that was granted to the application. It is unknown if this will cause any playability problems. Therefore, it is considered an ERROR.

Cause

This condition is normally caused during authoring of the image.

Solution

The image must be re-authored.

Type:	Blu-ray
Reference:	Blu-ray Specifications, Section 3-2: BD-Java Specifications
Default Program Action:	Error

Rule ID: 1650

XML parse error

An error occurred while parsing a Blu-ray XML file.

Background

Prior to analyzing the contents of an XML file, the EclipseSuite tools make sure that the file conforms to the XML specifications. Any error encountered during this process is reported with this rule. Note, however, that parsing the file does not mean that the file is being validated to a specific schema. The file is being checked to make sure that the XML document is well formed according to XML. There are separate rules that will be triggered when the file is validated against a schema.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will display more details about the error with the following message.

[*Filename*], '[*XML Error Description*]'. **Line:** [*Line #*], **Col:** "[*Col. #*]"

This message identifies the XML file that is being parsed. It also displays the error description as well as the line and numbers within the file where the failure occurred.

This error can occur on Manifest files, Playlist files and Advanced Resource files.

Severity

This rule indicates that the file does not conform to the basic rules of XML formatting. Therefore, it is considered an ERROR since it could cause systems to fail when trying to read its contents.

Cause

This problem is typically caused by the authoring system that created the image.

Solution

Since this is a generic error that is triggered when any part of the file does not conform to the XML format, it is impossible to predict if it can be corrected.

There may be conditions that can be ignored while others that may be fatal. It is possible that the image may have to be re-authored in order to correct the problem. Contact Eclipse Customer Support for further assistance.

Type:	HD DVD
Reference:	N/A
Default Program Action:	Error

Rule ID: 1508

XML Schema violation

A BD XML file failed the schema validation.

Background

When analyzing a BDCMF image, the EclipseSuite tools will attempt to validate all XML files that are part of the image. In order to perform this validation, the XML Schema files must be present in the same directory from which the EclipseSuite programs are being executed.

On a Blu-ray image, the files BDCMF.CMF and AACS1.DAT files will be validated.

Additional Info

When this rule is triggered, the **Additional Info** column in the Analysis will identify the XML file that failed validation and details about the reason why.

XML file '[*XML filename*]' missing required element '[*element*]'

This message is displayed when the specified XML element is not found in the XML file being validated.

XML file '[*XML filename*]' contains element '[*element*]' not defined in schema file '[*schema filename*]'

This message is displayed when the specified element is found in the XML file being validated but the element is not defined in the schema file.

Severity

This rule is triggered when any required XML element is missing or is undefined according to the schema file. Since this can apply to many XML elements, this rule is considered a WARNING. Elements that are present but not defined in scheme typically do not cause any problems. However, a missing required element should be considered serious.

Cause

This problem is typically caused by the authoring system that created the image.

Solution

If the rule is being triggered due to an 'extra' element that is not defined by the schema, then this should not be a problem. If the image is copied using ImageCopy, any 'extra' elements not defined by the schema will be removed. However, if the problem occurs because of a missing element, then the image may have to go back to authoring to be corrected.

Type:	Other
Reference:	N/A
Default Program Action:	Warning

Rule ID: 1516

ImageArchive BD

ImageArchive BD is a fast, secure, and reliable archiving program that allows the creation of Type C images from stored replicas.

Automatic

ImageArchive BD allows you to create Blu-ray archives without any additional steps to your process. During your normal CC signing process, ImageArchive BD automatically stores required data into the ImageArchive database. When you need to restore an image, ImageCopy can automatically find the archive record, and merge it with the encrypted user data from a saved replica to create a Type-C image ready for mastering. No AACS decryption or encryption is necessary.

Secure

ImageArchive BD can make Type-C images only from replicas that have been made in your premastering process, in your factory. And, since the ImageArchive database contains critical and sensitive AACS information, the archive database is securely encrypted. The restore process restricted through the use of Smartcard access.

Fast and Simple

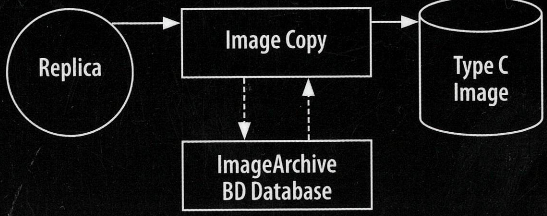
The restore process couldn't be simpler. Just select the restore replica as the source in ImageCopy BD, ImageCopy determines if the disc is a valid archive, and the original Type-C image is recreated. The process is as fast as current BD drives can read (currently 12X). No need to spend hours writing and reading images to and from recordable media or tape.

Reliable

Traditional tape and recordable media-based archive solutions suffer from reliability concerns: did you archive the right files; will the media be readable when you need to restore it in several years; will a compatible tape drive still be available? ImageArchive eliminates these questions. A replica is a strong storage format because the data is stamped in a metal layer and the data protected by a robust error recovery scheme. No need to worry about dye or magnetic degradation. A replica will always contain the files you need and the Eclipse ImageArchive BD system will always restore the image to the current BDCMF version. It's simple and cheap to keep multiple copies of archive replicas. With ImageArchive BD you will always have a usable archive on hand.

Cost Effective

HDD and tape-based archives are expensive, slow, and require system management. Replica-based archiving requires less then 1MB of storage per image and an archive disc can be created in one cycle of your replication press. Stop wasting valuable resources on time consuming and expensive magnetic media archives. ImageArchive BD takes advantage of readily available and inexpensive discs to eliminate the need for tape or hard disk based archive copies of images.



Tele + 1-925-224-8880 • www.eclipsedata.com • Fax + 1-925-224-8881

ECLIPSE
DATA TECHNOLOGIES